S. HRG. 108–925

THE 9/11 COMMISSION AND RECOMMENDATIONS FOR THE FUTURE OF FEDERAL LAW ENFORCEMENT AND BORDER SECURITY

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

AUGUST 19, 2004

Serial No. J–108–92

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

96–459 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

CHARLES E. GRASSLEY, Iowa	PATRICK J. LEAHY, Vermont
ARLEN SPECTER, Pennsylvania	EDWARD M. KENNEDY, Massachusetts
JON KYL, Arizona	JOSEPH R. BIDEN, JR., Delaware
MIKE DEWINE, Ohio	HERBERT KOHL, Wisconsin
JEFF SESSIONS, Alabama	DIANNE FEINSTEIN, California
LINDSEY O. GRAHAM, South Carolina	RUSSELL D. FEINGOLD, Wisconsin
LARRY E. CRAIG, Idaho	CHARLES E. SCHUMER, New York
SAXBY CHAMBLISS, Georgia	RICHARD J. DURBIN, Illinois
JOHN CORNYN, Texas	JOHN EDWARDS, North Carolina

BRUCE ARTIM, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS AND ANSWERS

SUBMISSIONS FOR THE RECORD

THE 9/11 COMMISSION AND RECOMMENDATIONS FOR THE FUTURE OF FEDERAL LAW ENFORCEMENT AND BORDER SECURITY

THURSDAY, AUGUST 19, 2004

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 9:32 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, Chairman of the Committee, presiding.

Present: Senators Hatch, DeWine, Chambliss, Cornyn, Leahy, Kennedy, Kohl, Feingold, and Schumer.

Chairman HATCH. We are ready to go here. I think we will have all our panelists come up to the table so that when we ask questions, we can ask everybody.

Senator LEAHY. But if we do that, Mr. Chairman, we are going to need more than—I think it would be almost—well, I think we would be rightly criticized if we then spent just the same few minutes each Senator Cornyn, myself or anybody else might have, and spread it across four instead of across two.

Chairman HATCH. Well, let's see what we can do.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Chairman HATCH. Let me just begin here by adding my voice to those who have expressed their appreciation to the members of the 9/11 Commission and their staff for their hard work in putting together a thorough report that includes many thoughtful recommendations.

I want to thank you, Senator Gorton, and you, Representative Hamilton. We know how hard you have worked to get this all done, and we have chatted with both of you extensively.

We also owe a debt of gratitude to all of the witnesses who appeared before the Commission, especially the representatives of families of those who perished in the horrific and unjustified attacks of nearly 3 years ago.

The first responsibility of government is to protect its citizens and we must never shy away from that duty. Today, the Judiciary Committee begins its discussion of the portions of the 9/11 Commission's report and recommendations that relate to areas under our jurisdiction, such as border security and the role of the FBI in the field of counterintelligence.

Our colleagues on the Governmental Affairs Committee, led by Senators Collins and Lieberman, have asked for our Committee's perspective on matters within our expertise, and I want to thank them for that.

In addition to those recommendations that are designed to help our law enforcement and homeland security agencies identify, thwart and apprehend terrorists, we on the Senate Judiciary Committee have a role in implementing and overseeing any recommendations aimed at protecting our civil liberties. I expect, for example, that today's hearing will help us gain a better understanding of the Commission's recommendation calling for the creation of a new civil liberties board.

Similarly, we must take to heart the Commission's recommendation with respect to our obligation to provide humane treatment for those detained as suspected or captured terrorists. The abuse of prisoners such as occurred at Abu Ghraib is contemptible, as well as counter-productive to our efforts to stop Islamist terrorism at its countries of origin.

Much attention has been focused on now-famous organizational chart on page 413 of the Commission report proposing the National Intelligence Director, the National Counterterrorism Center, and three dual-hatted deputies. As significant as the debate today over the structural issues is, it must not be allowed to crowd out an equally important policy discussion of those recommendations that urge America to stand up for and defend our core values and ideals with our foreign neighbors, and work to bring about long-term changes in the underlying economic and political conditions that foster Islamist terrorism in certain regions.

We must not be under any illusion that we can reach accommodations with Islamist terrorist organizations like al Qaeda. The Commission found that these groups do not hold views, quote, "with which Americans can bargain or negotiate...there is no common ground—not even respect for life—on which to begin a dialogue...[They] can only be destroyed or utterly isolated," unquote.

The deadly attacks on 9/11 required our country to adopt new laws to protect the public. I find constructive the Commission's observation that, quote, "a full and informed public debate on the PATRIOT Act would be healthy," unquote. In this regard, I would note that the Commission also found that "some executive actions that have been criticized are unrelated to the PATRIOT Act. The provisions that facilitate the sharing of information among intelligence agencies and between law enforcement and intelligence appear, on balance, to be beneficial," unquote.

The 9/11 Commission report documents the negative repercussions of the so-called wall that existed before enactment of the PATRIOT Act between intelligence and criminal investigators. Even if the Commission is accurate in its assessment that the July 1995 procedures establishing the wall by Attorney General Reno, quote, "were almost immediately misunderstood and misapplied," unquote, there can be no doubt, as Chapter 8 of the report lays out in great detail, that creation of the wall between intelligence and criminal investigators impeded rigorous following of leads that may have prevented the 9/11 attacks.

The Commission's report catalogs that on August 29, 2001, one frustrated FBI criminal investigator prophetically e-mailed across the wall to an FBI intelligence officer the following message after being denied the ability to access and use information about one key al Qaeda operative, quote, "...someday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain problems," unquote.

Never were more truer words written, but our job is to learn from our past mistakes in order to protect the American public in the future. If we carefully review the lessons contained in the 9/11 Commission report and fairly evaluate its recommendations, we will be able to marshal our resources and carry out our counterterrorism programs more effectively and reduce the risk of terrorist attacks against Americans at home and abroad.

For example, the Commission's report compellingly demonstrates the importance of border security and tracking international travelers. Under Secretary Hutchinson will help us understand the administration's views in this critical area.

Also of great interest to the Judiciary Committee is the Commission's recommendation relating to the future of the FBI in the war against terrorism. The 9/11 Commission report found that the FBI and Director Mueller have cooperated with the Commission. Recently, the FBI issued its formal response to the Commission's recommendations and in each instance was either implementing those recommendations or reexamining its current policy in light of the recommendations.

I would like to commend President Bush for his leadership in making certain that the key senior administration officials are giving the bipartisan 9/11 Commission report the respect and consideration that it merits and deserves.

It appears to me that, by and large, all of the committees in the House and Senate are attempting to approach the report in a bipartisan manner, despite the fact that we are deep into the election cycle and despite the fact that some of the Commission's recommendations are somewhat complex and controversial, such as those pertaining to changes in Congressional oversight of terrorism programs.

I hope that this spirit of bipartisanship continues this morning so that we can go about the serious business of adopting the set of policies and laws that best protects the American public from terrorism, while preserving our traditional rights and liberties as American citizens.

So I want to express my gratitude to all four of you being here—you two members of the Commission who have served so well and have given so much time to committees up here on Capitol Hill and have, I think, written an excellent report, for the work that the FBI does and, of course, Homeland Security does, represented by Ms. Baginski and Asa Hutchinson. I just want to tell you how grateful we are to have all of you here.

We will put your full statements in the record. I notice they are rather long. We would like you to summarize so that we have enough time for questions here today.

[The prepared statement of Senator Hatch appears as a submission for the record.]

So we will turn to Senator Leahy, and then we will turn to the witnesses.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Well, thank you, Mr. Chairman. I am glad you are having this hearing and I thank you for accommodating schedules so we could do it.

I am glad to see all the witnesses, especially my old friends Lee Hamilton and Slade Gorton. I had a chance to talk with both of them, although for months I felt as though they had never left because I would see them everyday on television.

I think that as the Commission's Chair and Vice Chair, Governor Kean and Congressman Hamilton offered extraordinary leadership, leadership in the highest traditions of our great country in guiding the investigation through difficult shoals and bringing the Commission not only to constructive, but unanimous findings and recommendations.

I have also heard the high praise that you and the other commissioners have had for the Commission staff. I join you in that praise. The report you have produced is an exceptional product and deserves the Nation's attention and deserves the Congress' prompt consideration.

Senator Gorton, I was so proud of many of the comments you made, but especially when you remarked that the commissioners checked their politics at the door. I think the quality of the Commission's report bears out what you had said.

Working in this non-partisan fashion, the 9/11 Commission has given us a chance for a fresh start in tackling the issues the report has identified. We shouldn't squander that chance. We should use the Commission as our model. After all, the terrorists don't attack Democrats or Republicans or independents. When they strike, they attack all Americans. I know my friend, Asa Hutchinson, has said very similar things in the past, and he and Ms. Baginski know this very, very well.

I also want to commend the tireless efforts of the families and survivors who fought so hard to ensure that this Commission was established. Like the commissioners, the victims groups put partisanship aside and they pushed for an open, deliberative and accountable investigation, moving us forward in a constructive manner to better protect this Nation. Many of the victims groups are here today. I want to thank them, I want to welcome them.

I might ask, Mr. Chairman, for consent to submit for the record the written statement of Donald Goodrich, of Bennington, Vermont.

Chairman HATCH. Without objection.

Senator LEAHY. He lost his son, Pete, on September 11th and he has come to work closely with me on victims issues. I want to express my deep appreciation to him.

We can't overstate the importance of oversight. The Commission deserves our praise for fighting for full access to documents and official testimony, and for acknowledging in its final report the importance of open government. They stated that secrecy can harm

oversight and note that democracy's best oversight mechanism is public disclosure.

We are going to focus on two areas of great significance—FBI reform and border security. Both are topics well-known to this a Committee and have been of particular concern to me. My home State of Vermont shares 90 miles of our international border with Canada and I know the challenges faced there.

The attacks of 9/11 did not create the problems the Commission has identified; it simply brought them into sharp relief. As someone who comes from a law enforcement background, several of them are problems that have concerned me for some time, and I know they concern others on this Committee from both sides of the aisle. Addressing some of these deficiencies was my first priority when I was Chairman for a few months before September 11th.

During our hearings that summer, it was already clear that the FBI over the years has lost its way on some of the fundamentals, the ABCs, starting with accountability; basic tools like computers, technology and translators; and culture issues, like the treatment of whistleblowers and a resistance to share information outside the Bureau.

We began bipartisan hearings on reforming the FBI just weeks before September 11th, and the new FBI Director pledged to make the changes necessary.

The Director has made significant progress on several fronts, but the Commission's report strikes several familiar chords, showing that there is much ground yet to cover before we can say that the FBI is as effective as Americans need the Bureau to be in preventing and combatting terrorism.

We continued the hearings on FBI reform after September 11th. We sharpened our focus on the relevance of these longstanding problems. Our inquiry constituted the most intensive FBI oversight in many years and generated wide-ranging recommendations. The Commission report identified many of the same failures within the FBI that we had highlighted in those hearings. It recognizes, as do I, that Director Mueller has already taken certain steps to solve structural problems and that he is striving to change the culture within the Bureau. These are important steps, but it also points out that we have to institutionalize these changes or they will die on the vine, as they have in the past, when you have lapses in leadership or oversight.

There are two particular areas that gravely concern me—and, Ms. Baginski, I will be going into this later—the FBI's foreign language translation program and its information technology system. These are the nuts and bolts of effective law enforcement and counterintelligence, but we know in the months leading up to September 11, 2001, they were in sorry shape. Three years later, and millions and millions of dollars later, we want to know what progress has been made.

Ms. Baginski has said recently she was optimistic about the status of the FBI's foreign translation program. I hope you have some good news for us today because last spring, despite claims of near real-time translation of wiretaps, the FBI could not state with any certainty how much time passes between the time a telephone call is taped and when it is translated. There is still a vast backlog, for

example, of material needing to be translated. The FBI sought an unprecedented number of new FISA wiretaps last year. I have to ask, how does this impact their resources?

The FBI longstanding problems of mastering the computer technology that is essential to modern-day law enforcement has been another great failing. The Trilogy solution that the FBI said would be the answer to the computer problems has been a disaster. By now, two phases of Trilogy have been completed. All agents at least have their own computers and can send e-mails to one another, something my 12-year-old neighbor was able to do years ago. It is hardly a noteworthy accomplishment in the Information Age, especially $500 to $600 million later. My neighbor did it for a couple of hundred dollars.

What troubles me, however, is the FBI agents are still trying to connect the dots using pencil and paper. That is fine for kindergarten, but it is not fine for our FBI. The long anticipated virtual case file system which would put intelligence at the fingertips of the agents in the field is far behind schedule. It is vastly over budget. It should have been operational long ago, but the dates keep getting extended. In May, the Director assured us that it would be deployed by the end of the year. A month later, in June, we were told there would be further delays. At this rate, by the time it is finally implemented, it will be outdated. We should be working with state-of-the-art technology.

There are other critical areas that need reform within the FBI. Some we learned from the 9/11 Commission, some we learned from our own oversight efforts and reports by the DOJ Inspector General, but some have come to light only because of whistleblowers.

Senator Grassley and I spent a great deal of time listening to reports from whistleblowers because we believed they may provide us with information critical to our National security. As a result of Enron and related corporate scandals, I worked with Senator Grassley and others in Congress to give broad protection to whistleblowers in the private sector.

But so far, Congress has not acted to protect those who come forward from the FBI. The FBI Reform Act that Senator Grassley and I introduced in July of 2003 is drawn from the FBI Reform Act that had been unanimously approved by this Committee a year before. It has died on the Senate floor because of anonymous holds on the Republican side. It does address several outstanding problems in the Bureau, and acting on those reforms is long overdue.

Finally, I want to raise the question of State grants for homeland security funding. The 9/11 Commission recommended that homeland security assistance should be based strictly on an assessment of risks and security questions. I believe the real problem we face is a failure on the part of both the Congress and the administration to make enough of an overall commitment of resources to first responders.

Instead of making first responders the priority they should be, some have preferred to pit State against State for the inadequate Federal resources that are available. Rather than turning large States against small States, the needs of both should be recognized.

The Commission has rendered to history its careful reconstruction. The Commission has given to us the task of carefully consid-

ering its recommendations drawn from those events, recommendations that in several ways would help the FBI get back to mastering its ABCs. We owe our fellow citizens and the families of those whose lives were lost or forever changed by those attacks our full and respectful consideration of these findings and recommendations. But let me say one more time, every single American owes an enormous debt of gratitude to Congressman Hamilton, to Senator Gorton and all the other Commission members.

[The prepared statement of Senator Leahy appears as a submission for the record.]

Thank you, Mr. Chairman.

Chairman HATCH. Thank you, Senator.

We will start with Congressman Hamilton, and then Senator Gorton. We would like you to summarize, if you can. We will put all full statements into the record, and then hopefully we will have enough time for some questions.

So, Lee, we are happy to have you here. We welcome all four of you here. We are grateful for the service you have given and we look forward to hearing your testimony.

STATEMENT OF LEE HAMILTON, VICE CHAIR, 9/11 COMMISSION, WASHINGTON, D.C., AND SLADE GORTON, COMMISSIONER, 9/11 COMMISSION, WASHINGTON, D.C.

Mr. HAMILTON. Thank you very much, Chairman Hatch, Ranking Member Leahy and the other distinguished Senators of this Committee. We are very pleased to be before you today. I want to just mention that Chairman Kean, who deserves enormous credit for his leadership in this Commission, is not able to be with us today. But I am delighted to have joining me Senator Gorton, who made innumerable contributions to this report and served with extraordinary distinction. We are aware, of course, that August is not usually a month when you meet, and we are very grateful to you for your willingness to be here to hear our testimony.

What we will do is kind of alternate in summarizing our paragraphs, as the Chairman has indicated. You have asked us to discuss three topics—our findings and recommendations with regard to the FBI; secondly, border security; and, third, the PATRIOT Act. We will discuss each of these in turn.

Senator?

Mr. GORTON. The FBI has for several decades performed two important but related functions. First, it serves as our premier Federal law enforcement agency investigating possible violations of Federal criminal statutes and working with Federal prosecutors to develop and bring cases against violators of those laws.

Second, it is an important member of the intelligence community, collecting information on foreign intelligence or terrorist activities within the United States. That information can be used either for additional counterintelligence or counterterrorism investigation or to bring criminal prosecutions.

We focused on the FBI's performance as an intelligence agency combatting the al Qaeda threat within the United States before 9/11. And like the Joint Inquiry of the Senate and House Intelligence Committees before us, we found that performance seriously deficient.

Finally, when FBI agents did develop important information about possible terrorist-related activities, that information often did not get effectively communicated either within the FBI itself or in the intelligence community as a whole.

Within the FBI itself, communication of important information was hampered by the traditional case-oriented approach of the agency and the possessive case file mentality of FBI agents. As this Committee is only too familiar with the information technology problems that have hampered the FBI's ability to know what it knows for years, even when information was communicated from the field to headquarters, it didn't always come to the attention of the Director or other top officials who should have seen it.

This was the case in the now-famous incidents in the summer of 2001 of the Phoenix electronic communication about Middle Eastern immigrants in flight schools and the Minneapolis field office's report to headquarters about the arrest of Zacarias Moussaoui.

The other internal barrier to communication of intelligence information between the FBI intelligence officials and the FBI criminal agents and the Federal prosecutors was the wall between intelligence and law enforcement that developed in the 1980s and reinforced in the 1990s.

Through a combination of court decisions, pronouncements from the Department of Justice and its Office of Intelligence Policy and Review, and risk-averse interpretations of those pronouncements by the FBI, the flow of information between the intelligence and criminal sides of the FBI and the Justice Department was significantly choked off—a phenomenon that continued until after 9/11, when the Congress enacted the PATRIOT Act and when the Justice Department successfully appealed a FISA court decision that effectively reinstated the wall.

These failures in internal communications were exacerbated by a reluctance of the FBI to share information with its sister agencies in the intelligence community. The FBI, under the leadership of its current Director, Robert Mueller, has undertaken significant reforms to try to deal with these deficiencies and build a strong capability in intelligence and counterterrorism.

Because of the history of serious deficiencies and because of lingering doubts about whether the FBI can overcome its deep-seated law enforcement culture, the Commission gave serious consideration to proposals to move the FBI's intelligence operation to a new agency devoted exclusively to intelligence collection inside the United States, a variant of the British security service popularly known as MI–5.

We decided not to make such a recommendation for several reasons set forth in our report. Chief among them were the disadvantages of separating domestic intelligence from law enforcement and losing the collection resources of FBI field offices around the country, supplemented by their relationships with State and local law enforcement agencies.

Another major reason was civil liberties concerns that would arise from creating outside of the Justice Department an agency whose focus is on collecting information from and about American citizens, residents and visitors. We also believe that while the jury is still out on the ultimate success of the reforms initiated by Direc-

tor Mueller, the process he has started is promising, and many of the benefits that might be realized by creating a new agency will be achieved, we are convinced, if our important recommendations on restructuring the intelligence community, creation of a national counterterrorism center and a national intelligence director with real authority to coordinate and direct the activities of our intelligence agencies are implemented.

An FBI that is an integral part of the NCTC and is responsive to the leadership of the national intelligence director will work even more effectively with the CIA and other intelligence agencies, while retaining the law enforcement tools that continue to be an essential weapon in combatting terrorism.

What the Commission recommends, therefore, is that further steps be taken by the President, the Justice Department and the FBI itself to build on the reforms that have been undertaken already and to institutionalize those reforms so that the FBI is permanently transformed into an effective intelligence and counterterrorism agency. The goal, as our report states, is to create within the FBI a specialized and integrated national security workforce of agents, analysts, linguists and surveillance specialists who create a new FBI culture of expertise in national security and intelligence.

Mr. HAMILTON. On Border Patrol, I think our principal finding was a simple one, and that was that border security was not seen as a national security matter. We looked at it as a narcotics problem, illegal immigration, smuggling of weapons of mass destruction. But we simply did not exhibit a comparable level of concern about terrorists' ability to enter and stay in the United States.

Al Qaeda was very skillful in exploiting the gaps in our visa entry systems. They even set up their own passport office. They developed very good contacts with travel facilitators and were very effective in getting into the country.

The Commission found that many of the 19 hijackers were potentially vulnerable to detection by border authorities, for all kinds of reasons. Some made false statements on their visa applications, some lied, some violated the rules of immigration. One failed to enroll in school; two over-stayed their time. But neither the intelligence community nor the border security agencies nor the FBI had programs in place to analyze and act upon that intelligence on their travel tactics.

Since 9/11, we know that important steps have been taken to strengthen our border security. We spell them out in our statement. I will not go into those. The efforts have certainly made us safer, but not safe enough. As a Nation, we have not yet fully absorbed the lessons of 9/11 with respect to border security.

The terrorists are travelers; they are jet-setters in many ways. They have to leave safe havens, they have to travel clandestinely, they have to use evasive techniques, they have to alter travel documents. All of these things give us an opportunity to zero in on the terrorists. So we have recommended a broad strategy that combines terrorist travel intelligence, operations, law enforcement, in a strategy to intercept terrorists, find their travel facilitators and constrain their mobility.

Mr. GORTON. Front-line border agencies must not only obtain from the intelligence community on a real-time basis information on terrorists. They must also assist in collecting it. Consular officers and immigration inspectors, after all, are the people who encounter travelers and their documents. Specialists must be developed and deployed in consulates and at the border to detect terrorists through their travel practices, including their documents.

Technology has a vital role to play. Three years after 9/11, it has been more than enough time for border officials to integrate into their operations terrorist travel indicators that have been developed by the intelligence community. The intelligence community and the border security community have not been close partners in the past. This must change.

We also need an operational program to target terrorist travel facilitators, forgers, human smugglers, travel agencies and corrupt border officials. Some may be found here, but most will be found abroad. Disrupting them would seriously constrain terrorists' mobility. While there have been some successes in this area, intelligence far outstrips action. This problem illustrates the need for a national counterterrorism center.

Investigations of travel facilitators invariably raise complicated questions. Should a particular travel facilitator be arrested or should he be the subject of continued intelligence operations? In which country should he be arrested? A central planning authority is needed to bring the numerous agencies to the table and to decide on the best course of action.

Mr. HAMILTON. With regard to screening systems, we think the Government simply must accelerate its efforts to build a comprehensive biometric entry and exit screening system. The Congress has had an interest in that, but as a practical matter there hasn't been any funding until the end of 2002.

The new Department of Homeland Security, we believe, is emerging from its difficult start-up period, and we believe it is poised to move forward to implement Congress's mandate in this area. We stress four principles.

One is that the Department has to lead with a comprehensive screening system. We will have more to say about that, I am sure, in the Q and A period. It addresses the common problems, setting common standards with system-wide goals in mind.

Secondly, a biometric entry and exit screening system is just fundamental to intercepting terrorists, and its development should be accelerated. Each element of that system is very important. It must enable the border officials to access all relevant information about a traveler in order to assess the risk they may pose. We must know who is coming into this country. We must know people are who they say they are.

The third principle is that United States citizens should not be exempt from carrying biometric passports or other identities to be securely verified. And there should be a uniform program to speed known travelers so inspectors can focus their efforts on the ones that might pose greater risks.

Mr. GORTON. We need to dedicate a much greater effort to collaboration with foreign governments with respect to border security. This means more exchange of information about terrorists and

passports, and improved global passport design standards. Implicit in this recommendation is continued close cooperation with Mexico and Canada. One particularly important effort is to improve screening efforts prior to departure from foreign airports, especially in countries participating in the visa waiver program.

Mr. HAMILTON. Our law enforcement system has to send a message of welcome, tolerance and justice to members of the immigrant communities in the United States, fostering also a respect for the rule of law. Good immigration services are one way to reach out that is valuable, including for intelligence.

State and local law enforcement agencies need more training; they need to partner with Federal agencies so that they can cooperate more effectively in identifying terrorist suspects. We also need secure identification, and that should begin in the United States. We believe that the Federal Government should set standards for the issuance of birth certificates and sources of identification such as drivers' licenses. The bottom line is that our visa and border control systems must become an integral part of our counterterrorism intelligence system.

Mr. GORTON. The USA PATRIOT Act, passed in the wake of the 9/11 attacks, was substantially the product of this Committee. While a number of provisions of the Act were relatively non-controversial, updating existing authorities to take account of the digital age in which we now live, others are more far-reaching, granting to the FBI, the Department of Justice and other executive branch agencies important new authorities to use in combatting terrorism.

For this reason, the Congress chose to sunset many of the provisions of the Act at the end of next year. We know that this Committee and the House Committee on the Judiciary will be holding hearings to determine whether to extend these expiring provisions and whether to make additional changes in the law.

This Commission did not canvass the entire range of issues raised by the USA PATRIOT Act in detail. We have limited our specific recommendations with respect to the Act to those provisions that bear most directly on our mandate; i.e. those that relate to information-sharing in the intelligence and law enforcement communities. We believe that those provisions breaking down the wall that prevented the FBI from sharing intelligence information guaranteed under FISA with Federal prosecutors and allowing the Justice Department to share grand jury information with other intelligence and law enforcement agencies should be extended or made permanent. They are important in their own right and they have helped spur the increased sharing of information throughout the intelligence community that is vital to a successful counterterrorism program.

We made a general recommendation that applies not only to consideration of other provisions of the PATRIOT Act, but also to other legislative or regulatory proposals that may impinge on individual rights or liberties, including personal privacy. The burden in all cases should be on those proposing the restriction to show that the gains that will flow in terms of national security are real and substantial and that individual rights and liberties will be adequately protected. We recommend the establishment of appropriate

guidelines for such programs. We also recommend the establishment in the executive branch of an oversight office or board to be a watchdog to assure maximum protection of individual rights and liberties in those programs.

Let us conclude with what we said in our report. We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice and nothing is more likely to endanger American liberties than the success of terrorist attacks at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.

We are now pleased to answer your questions.

[The prepared statement of Messrs. Hamilton and Gorton appears as a submission for the record.]

Chairman HATCH. Thank you very much.

We want to thank you, Secretary Hutchinson, for being here. You have testified, I believe, 12 times so far before committees up on Capitol Hill here in this last short time, and we are grateful that you have been willing to come and testify here as well.

Senator LEAHY. Asa spends more time here now than when he was in the House.

Chairman HATCH. I don't think you have to take that kind of stuff.

[Laughter.]

STATEMENT OF ASA HUTCHINSON, UNDER SECRETARY FOR BORDER AND TRANSPORTATION SECURITY, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.

Mr. HUTCHINSON. Well, thank you, Chairman Hatch, Senator Leahy, members of the Committee. I would love to have an honorary seat somewhere here if I continue to testify, but it is always a privilege to be before this Committee.

As we approach the anniversary of the September 11 attacks, it is important to recognize that significant progress has been made. But we also understand there is a great need to do more, and I am grateful for the testimony of Congressman Hamilton and Senator Gorton, who have done such a terrific job with the 9/11 Commission. The recommendations in their testimony today will help us to drive forward many of the initiatives that the Department of Homeland Security has been engaged in.

I wanted to cover a couple of points that are covered in the Commission report and talk about some of the things we have done in this regard.

In its report, the Commission noted that vigorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. We certainly agree with this. Well over a year ago, the Department has worked in close cooperation with the FBI and others to track terrorist financing and to dismantle the sources of terrorist funding.

The Department's Immigration and Customs Enforcement, or ICE agents share all terrorist financing leads with the FBI under a memorandum of agreement with the Department of Justice. We have established a joint vetting unit to clear all investigations with any potential nexus to terrorist financing. We have also assigned

VerDate Aug 31 2005 15:22 Oct 22, 2008 Jkt 096459 PO 00000 Frm 00016 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\96459.TXT SJUD1 PsN: CMORC

321 ICE agents to the FBI's joint terrorism task forces, which is a very effective means of clearing information and enhancing cooperation.

ICE initiated the Cornerstone program, which focuses on the systems of financing that criminals, terrorists and alien smugglers use to earn, store and move their proceeds. To date, Cornerstone has recovered $348 million in illegal currency and made 1,800 arrests.

Another recommendation of the Commission was in reference to terrorist travel that was testified to previously, that we should combine terrorist travel intelligence, operations and law enforcement in a strategy to intercept terrorists and their facilitators as they go about their business. The Department has moved forward with this aggressively. There is more to be done.

Through the National Targeting Center, which is operated by Customs and Border Protection, we use a variety of information to identify potentially high-risk travelers and shipments that should have more scrutiny. We have the Automated Targeting System that allows us through the NTC to analyze raw intelligence and travel data and commercial data to pinpoint anomalies to help us to be able to flag those that might pose a risk. That is the foundation, of course, for the Container Security Initiative, which is the cargo side of our inspections. So that is the capacity to look at terrorist travel.

Secondly, we have our US–VISIT program that provides an important continuum of security that has improved our ability to target individuals, and hopefully to have the traveler files in place that the Commission has referred to. US–VISIT for the first time allows us to biometrically confirm the identity of foreign visitors as they enter our ports of entry. It has allowed us to freeze the identity of travelers, to positively match that identity with the individual's travel document and to determine over-stays.

We recognize the Commission's recommendation that this program be accelerated, and this Congress has given us some very strict deadlines. We have met the deadlines that have previously been provided to us. This year, we are looking at the 50 busiest land ports as our deadline. We intend to make the very aggressive deadlines Congress has given, but if there are ways to accelerate this and expand it, we certainly are open to those possibilities.

In the first 7 months of operation, US–VISIT processed nearly 7 million foreign national applicants for admission at our air and sea ports of entry. During that time, 674 individuals have been identified through biometrics alone as being the subject of a lookout. Of the 674 hits, 64 percent were for criminal violations and 36 percent were for immigration violations alone. We continue to develop the exit capacity in reference to that program, now relying upon biographic information for exit procedures.

Through US–VISIT, we caught a woman who had used a fraudulent visa to enter the United States over 60 times without being detected by standard biographic record checks. We also stopped a convicted rapist previously deported from the United States who had used nine different aliases and four dates of birth. US–VISIT enhances our ability to track criminal and terrorist travel. It also contains unprecedented privacy protections that are very important.

Those are the international travel components for the terrorists that may try to enter the U.S. We also, through TSA's no-fly and selectee lists, look at domestic travel. We have to enhance the capabilities in that arena that we are working on.

We also are concerned about our vast land borders that many of the Senators on this panel have raised issues concerning. The Commission's report refers to having the capacity to monitor and respond to intrusions across our border. That is the basis of the Arizona Border Control Initiative, in which we have utilized unmanned aerial vehicles, new technologies and new personnel assigned to that difficult border region.

The 9/11 Commission report recommends that the U.S. border security system should be integrated into a larger network of screening points. Integration, of course, is the main focus of the US–VISIT program that has brought together and made the databases speak to each other from the State Department, to our criminal databases, to our port of entry databases. We continue to expand that integration.

Our first responsibility is to make sure that the systems we are working on operate effectively, from US–VISIT, to our pilot program on transportation worker identification credentials, to our registered traveler program. But we also recognize the need to review all of these programs and coordinate them together because they all look at a whole range of biometrics and we want to be able to coordinate those. The Department is accelerating that effort as well.

Finally, on the USA PATRIOT Act, I would second the point that this has been a very helpful tool obviously to the FBI, but also to all who work in law enforcement. From a Department of Homeland Security standpoint, it has given us a greater capability to go after the bulk cash transfers of money that was previously a reporting violation, but now is a criminal offense. It also enhances the sharing of information between those in the intelligence community and the law enforcement side, breaking that wall down, that is helpful to our efforts as well. We are very focused on these initiatives. The Commission report will help us to push these forward even to a greater extent.

I want to thank the Committee for their leadership on these very important issues.

[The prepared statement of Mr. Hutchinson appears as a submission for the record.]

Chairman HATCH. Well, thank you, Secretary Hutchinson.

Ms. Baginski is the Executive Assistant Director of Intelligence for the Federal Bureau of Investigation. We are so grateful to have you here today, so we will take your testimony at this time.

STATEMENT OF MAUREEN A. BAGINSKI, EXECUTIVE ASSISTANT DIRECTOR, INTELLIGENCE, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, D.C.

Ms. BAGINSKI. Thank you, Mr. Chairman and distinguished members of the Committee, for the opportunity to appear before you to discuss the recommendations of the 9/11 Commission. The FBI applauds and is very grateful for the work of the Commission.

We are also grateful to the families for reminding us for whom and why we serve always.

We are pleased that the Commission has embraced the general direction of our reform, and we agree wholeheartedly that much work remains to be done to institutionalize that reform. We are committed to doing everything that we have to do to do that.

Intelligence, which we define as vital information about those who would do us harm, is a powerful tool in defense of the Nation. In using that tool comes great responsibility: first, the responsibility for producing and sharing that information, and the responsibility for its accuracy; second, the responsibility for ensuring the protection of the rights of U.S. citizens as it is produced and collected; and, third, the responsibility for using the Nation's resources responsibly as you develop capabilities to do the intelligence mission.

If intelligence is vital information about those who would do us harm, then the only true value of intelligence is in the eyes of the users of intelligence. The only true measure of the value of intelligence is whether or not it helps someone make a better decision. So in the eyes of the producer is not how we measure the value of intelligence.

When we think about the range of decisiomakers that are necessary to defend our Nation, you could think about them as ranging from the President to the patrolman. And those of us with the responsibility of producing and sharing information must make sure that they are networked together with information that allows them to act in defense of the country. In the end, that is what intelligence really is.

This is not the responsibility, as you say and know, of the Federal family alone. We are part of many networks. We are part of a Federal network. We are part of an intelligence community. We are part of the law enforcement community. We are part of 800,000 State, local and tribal police officers who together, everyday, protect the Nation on the front lines. They will be the first to encounter the threat and they will be the first to defend against that threat.

So everything that we have done in the FBI for intelligence has been about getting our own internal act together so that we can be the best node possible on this network, the network itself is only going to be as effective as its individual members coming together in that network.

My responsibility at the FBI has been to take charge of creating an enterprise-wide intelligence capability under the leadership of Director Mueller. Intelligence reform, I think as the findings of the Commission have proven, at the FBI has been a very evolutionary process, starting first immediately in the aftermath of 9/11 very focused on counterterrorism, very focused on getting the information out and producing strategic analysis, and then finally culminating in the Director's decision to create an Executive Assistant Director for Intelligence. And I was very, very proud to take such a position last year, May of 2003. As I said, all of our efforts have been about getting our own internal act together, and we still do have work to do.

In the interest of time, I only want to share with you the core principles on which we have built that, and the first thought is a very important one and that is that intelligence is the job of the entire FBI, not just the job of my organization. If we are to do it correctly, then our training, our security, all of the components that make up the FBI must be as optimized for its intelligence mission as it is for its law enforcement mission.

After that core principle come four. The first is the integration of intelligence and law enforcement operations. Intelligence is best when it is informed by an operational view. I think I bring my bias to that largely from my experience in the Department of Defense, where intelligence was always very integrated with military operations.

Secondly, at the same time that you want production integrated, you do want an independent requirement and collection management process. By that, I simply mean an independent authority setting priorities, looking at what you are doing against those priorities, consistently identifying gaps and developing the strategies to develop sources to fill those gaps. That is the responsibility of my organization.

Third, centralized management and distributed execution. The power of the FBI intelligence capability is in its 56 field offices and 400 resident agencies. It is in those numbers that are out there. So, it is getting them to have a shared view of the threat; a single set of operating processes, policies and procedures; the resources to do that work; the IT to connect them; the humans to do the analysis; and allowing that power to perform.

Fourth, focused strategic analysis. If we spend all of our time doing current reporting, we will be working the urgent, and my job is to make sure we are also working the important.

In the interest of time, I don't want to go over the accomplishments, although we are very proud of all of them. I would just focus on a couple to get to your opening statements because I think they are, in fact, very important and we share many of your concerns.

In terms of information-sharing, we have tripled the amount of raw intelligence reporting that we have done already this year over last year, and we have doubled the number of assessments that we have provided.

Senator LEAHY. Provided to whom?

Ms. BAGINSKI. That we have provided to the larger intelligence community, and also to the Congress and to State and local law enforcement.

Also on the cultural side, you are right; there is much work to do on culture. And that is not a light switch; that takes time to work through. There are two critical things that the Director has championed, and the first is changing the performance evaluations of the agents to include a critical element that grades them against source development and intelligence production; and, finally, the proposal for an intelligence officer certification that requires intelligence officer certification for all of our agents before they could become ASACs or section chiefs, the first SES level at headquarters.

I could detail more achievements and more accomplishments. We think we are on a good path. We think the Commission is also right; we have much work to do. With that, we look forward to your questions.

[The prepared statement of Ms. Baginski appears as a submission for the record.]

Chairman HATCH. Well, thank you so much. We appreciate all four of you and your statements and we are encouraged by those statements.

Let me ask a question to both Commissioners in this first round here. Although the Commission's rejection of the MI–5 model was conditioned upon adoption of the panel's other recommendations, such as the creation of the counterterrorism center and the national intelligence director, Congressman Hamilton, you have personally voiced strong objections to the MI–5 model, regardless of the enactment of these other measures. I would like to know what is that.

Senator Gorton, I am interested to hear your views, as well, on that.

Mr. HAMILTON. Senator Hatch, we looked at MI–5 because of the record the FBI had in the lead-up to 9/11 was not impressive. We were intrigued by it. We flirted with it a little bit, but we soundly rejected it in the end. We rejected it, I think, for several reasons.

One was the concern for civil liberties. We think the FBI does have a tradition of rule of law, protection of civil liberties. We were afraid setting up another independent domestic intelligence without that tradition would not be helpful.

Secondly, we think the FBI is moving in the right direction now to correct the deficiencies, and to set up an MI–5 would be terribly disruptive, would take a long time, would be very costly—you would have to set up separate training facilities and bring new agents in and all the rest of it—and would not be helpful at this point in time. So the MI–5 was rejected.

Interestingly enough, when we talked with the Brits about this, they didn't even think an MI–5 was a good idea for the United States because the two countries are so very, very different. So we rejected that completely and emphasized instead the importance of focusing on institutionalizing the reforms that are underway.

Mr. GORTON. I would simply emphasize what Lee has said. I think one of our most fascinating and delightful interviews was with the head of MI–5. She said, among other things, there, her relationships are with exactly 56 chief constables in the United Kingdom, all of whom she knows personally. Here in the United States, of course, we have 10, 15,000 different police agencies, many of which have developed good relationships with the FBI agencies in their given areas. There are just too many differences between the United States and the United Kingdom.

And you shouldn't underestimate, of course, the dislocation of creating an entirely new agency, the potential of one further stovepipe, one further agency not to communicate with others. But I think the primary reasons were positive, were the significant progress that we believe that the FBI has made under Bob Mueller in correcting many of the failures that led up to 9/11.

Mr. HAMILTON. We see an important advantage in the FBI's ability to link law enforcement and intelligence. They are not separate. You cannot separate them completely. What the investigator finds out here with regard to intelligence can be helpful to the criminal prosecutor. What the criminal prosecutor finds out in his investigation can be helpful on the intelligence side. That link, that synergy is important.

Chairman HATCH. Let me just ask one other question.

Vice Chairman Hamilton, in prior testimony on this subject you have suggested that new legislation on information-sharing and the reforms at the FBI may not be necessary, if I interpret it correctly, so long as the current Director takes steps to institutionalize his reforms or the President issues appropriate executive orders.

Could you elaborate on those observations on the merits of entrusting some of these recommendations to the executive branch?

Mr. HAMILTON. Well, what we found, I think, as we looked at the problem of sharing information—and that really was critical for us. We think 9/11 came about, in part, because we did not do as good a job as we should have in sharing information. Whereas many of our intelligence agencies are very good at what they do, they nonetheless have a kind of a restricted view of the world and we think the sharing was critically important.

Now, the whole question of integrating information systems, the reform of them, the improvement of them, cannot be done by a single agency or even a single department. What you need is integration, and that can only be done across the Government, and when you are seeking action across the Government, you have to have the President do it. I don't know any other way to get it done.

So we call upon the President here to lead a major effort in the Government to develop common standards, common practices, common approaches to the information system. I don't think we considered that a legislative matter. We think it really has to be done by the President, and the benefits of it are just enormous if you can get that free flow of information flowing across these stovepipes that we have.

Mr. GORTON. Bob Mueller had one tremendous accidental advantage. He became the head of the FBI one week before 9/11. He had no intellectual or emotional investment in the way business had been done prior to 9/11 and that gave him a very great ability to make dramatic changes.

We had two concerns, however—the very strong culture of the FBI itself which creates internal resistance to major change, and the fact that no individual is going to head it forever, and we have no idea who his successor may be. So we want these very positive changes to be institutionalized.

I think a major reason that we said that this could be done by executive order is to freeze a particular structure in the law makes it extremely difficult to change. Whether every element of an original change through executive order is a hundred percent correct is certainly a matter which one can question, and there is a somewhat easier facility to make adjustments if the reforms are done by executive order. We do think they need to be institutionalized and can't just be left up to the Bureau itself, but we don't think it absolutely necessary that they be put into statute.

Chairman HATCH. Thank you, Senator. My time is up.

Senator Leahy.

Senator LEAHY. Well, thank you, and thank you again to the four witnesses. To follow up on what Senator Gorton said. The institutionalizing of some of these reforms is very necessary. We sometimes rely too much on ad hominem reform, which simply allows those within the bureaucracy who don't want a reform to hunker down and just wait for the person who feels that way to leave, because ultimately people in these positions come and go.

Congressman Hamilton, again, please tell Governor Kean also of our great respect for what he has done.

Under Secretary Hutchinson, we talk about how we get information back and forth, and if I might be allowed just a little bit of parochial bragging, you and I visited the Law Enforcement Support Center, the LESC, in Williston, Vermont, the Nation's primary database and search engine for criminal aliens.

As you know, whether it is two o'clock on a Sunday morning in the middle of a three-foot—and that is not an exaggeration—snowfall or in the middle of a sunny summer afternoon, they are operating. They answer 750,000 queries a year from law enforcement in 50 States. They answer them within 15 minutes or sooner.

Would you say this is something that we could look at as a model for talking about how you do real-time sharing.

Mr. HUTCHINSON. I think the Law Enforcement Support Center in Vermont is an unheralded example of some of the things that are being done right in sharing information with our State and local officers. The fact that the men and women there at the facility in Vermont are loading into the immigration file of the NCIC, National Crime Information System, allows all of that information on immigration violators to be available to local law enforcement.

As a result of that effort, we have increased the detainers that have been lodged, the number of absconder files that are entered into the system, and we have actually decreased the number of alien absconders that are in this country. So we certainly applaud that effort and we expect great results in the future on it.

Senator LEAHY. Congressman Hamilton and Senator Gorton, I am reading from your final recommendations with respect to the FBI. You say that the Congress should make sure funding is available to accelerate the expansion of secure facilities in FBI field offices so as to increase their ability to use secure e-mail systems in classified intelligence product exchanges.

We have already given the FBI hundreds of millions of dollars to upgrade its information technology systems to bring the FBI into the 21st century. I have spoken before about how prior to 9/11 they were deciding how they could put agents on airplanes to bring photographs of suspected hijackers to different parts of the country, something any grade school kid could have e-mailed to someone else.

We spent hundreds of millions of dollars on Trilogy. It is way over budget. It is nowhere near completion. Some think it never will be. I wonder if money is the only thing because you also recommend that the Congress should monitor whether the FBI's information-sharing principles are implemented in practice.

But, for the Congress to do this, they have got to get answers from the Department of Justice and we don't get them, whether it is Republican Senators or Democratic Senators asking. I can give you a list of things that have been asked for years. They just don't bother to answer or send non-answers.

If it sounds like I am frustrated, I am, because we have shown a willingness to authorize the money—and I am also on the Appropriations Committee—and the willingness to appropriate the money for all of this, yet we have no way of finding out what goes wrong after we appropriate it.

How do we get this information? What is your recommendation?

Mr. GORTON. I think if there were an easy answer to that question, Senator Leahy, you would have long since come up with it. Obviously, it is not only with the FBI and the Department of Justice that hundreds of millions of dollars have been appropriated to bring them into the information age, but many other departments as well.

Going beyond our recommendation, perhaps some of the concerns are with the elaborate nature of the acquisition process in the Federal Government. The information age revolution goes so fast that by the time we go through our normal procurement processes, we are in the next generation. That may be one thing to look at.

We didn't attempt to become experts in procurement policies or the like. We saw a lack of an ability within an agency to share information and have recommended changes. You also may note in another part of our report we talk about Congressional oversight and show deep concern with the fact that Asa here must spend a huge amount of his time—you have said how many times he has come to this Committee.

Senator LEAHY. We were referring to all committees.

Mr. GORTON. Yes, 88 committees and subcommittees that the Department of Homeland Security must report to. I suspect that Congressional oversight would probably be sharper if it were somewhat more limited.

Senator LEAHY. In this Committee, somebody once said, I think, Dracula fears holy water less than the Attorney General fears coming to this Committee. We don't see him, and we like him. I mean, we are all friends with him and we all served with him, but getting answers is very, very difficult.

I will give you one example. Three years ago, in the PATRIOT Act, we had a requirement, not a request, but a requirement that the Attorney General prepare a comprehensive report on the FBI's translation program. We have never gotten it, even though that is vital to our understanding of virtually every piece of intelligence information from the Middle East.

I know this particular section very well; I wrote it. The PATRIOT Act required it because ensuring the FBI's translation program is working to its potential is important to national security. There is an awful lot of data out there that is not translated. We have a huge ability with FISA, without going into the nature of some of our intelligence-gathering abilities, to get all this information, but then it sits there untranslated. We can't even get something that is required by law from the Attorney General that has been required for 3 years to tell us what is happening.

What do we do about that?

Mr. GORTON. Ultimately, you have the purse strings. That is the ultimate control.

Senator LEAHY. Thank you. My time is up. I will come back later.

Chairman HATCH. Thank you, Senator.

We will turn to Senator Cornyn, who was here first.

Senator CORNYN. Thank you, Mr. Chairman. Thanks to the panel for being here. I have two questions, as time permits. One has to do with continuity of Government and the other has to do with border security, and I would like to direct my first question to Congressman Hamilton and Senator Gorton.

It has been almost 3 years since Flight 93 was diverted and crashed in a place other than which it was originally intended to crash, and that is possibly the United States Capitol or at the White House, potentially decapitating the United States Government. Since that time, a bipartisan Commission and a joint venture of the Brookings Institution and the American Enterprise Institute have come up with some very good, in my opinion, recommendations for the Congress to undertake with regard to presidential transition and Congressional continuity. But so far, we have had perhaps even less success than the Government has had generally in improving our situation since 9/11 in this area.

I would ask perhaps, Congressman Hamilton, for you to first address that, and then Senator Gorton. How urgent do you believe it is for Congress to deal with the matter of governmental continuity, where the alternative if we don't do anything—and there is a successful decapitation, debilitation of the Congress—the alternative is essentially martial law?

Mr. HAMILTON. Senator, we did not address your specific proposal with regard to a constitutional amendment, nor did we delve greatly into the question of continuity of Government. We had a statutory mandate. We interpreted that mandate fairly carefully or strictly, and we did not think that it was clear that we should get into the continuity of Government question. We know it is a major concern here in the Congress, as it should be. So we cannot speak as a Commission with regard to your particular proposal.

We do think that you are putting your finger on a very, very important problem, however, and in the report we address the question of transition. We think that the country is most vulnerable, or very vulnerable perhaps I should say, during a period of transition of Government. And we make some recommendations with respect to requiring a President-elect to submit nominees in the national security area, and for the Senate to act to accept or reject those nominations within a 30-day period, because we are concerned about that transition period.

Now, your proposal has a lot of similarities with that. It is broader than ours. You speak about all the Cabinet members, as I recall, in your proposal, not just the national security proposals. So we are very receptive to proposals on continuity of Government, but we did not endorse any particular approach to them. We do appreciate your initiative.

Mr. GORTON. We were not able to determine with absolute certainty the target at which Flight 93 was aimed, but I think all of

us believe that it was much more likely than not that it was the Capitol. The basis of your concern is well taken.

As Lee has said, we deal with maybe the first cousin of your proposal in dealing with transition. We were particularly struck by the attack on the Cole which took place in late October of the year 2000. Within a couple of weeks, there was a preliminary determination of responsibility. A final determination literally took years, but in that transition time neither administration felt certain enough or concerned enough to deal with it and it went entirely unanswered.

That was the reason, or a major reason that we went into the transition to try to get national security officers into place as quickly as possible. You have taken a step beyond that and gone beyond anything we thought about in suggesting that the sitting President make the nominations for his successor. I think that is an absolutely intriguing idea, as are your ideas with respect to the continuity of Government.

We looked at our charge and we simply didn't get into it. But is it a vitally important issue and one that we think should be given serious consideration by the Congress? The answer to that is a total affirmative.

Senator CORNYN. Thank you for your answers. I do understand it was not perhaps within the scope of your Commission, but I do appreciate your responses. I wish I could claim originality, but there are a lot of very smart and very dedicated people who have made some recommendations which I have tried to bring forward together with others in Congress to address those.

Secretary Hutchinson, I want to tell you what an outstanding job I think you and the Secretary have done in trying to address the border security concerns we have. But I can tell you, as you know and as we have discussed, as a Texan, with a 1,200-mile border with Mexico and a southern border of Mexico leading down to Central America, one of the most porous in the country, we still have a long way to go. And I know you recognize that.

I would like to ask you specifically about how do we conserve our resources, or I should say direct our resources in a way that goes after those who would come across our borders with malicious intent from those who want to come across our borders with benign, perhaps even beneficial intentions.

I speak specifically of whether you think a temporary worker program, something that would deal not necessarily with people who are just wanting to come, but even people who are already here and working in our economy—the last estimate I heard is about 6 million in that workforce—do you think a worker program and immigration reform need to be coupled with our efforts at border security?

Mr. HUTCHINSON. Thank you, Senator Cornyn, particularly for your leadership and push on a number of border security issues.

In reference to the borders, first of all, I think it is important that we understand the difference between those that come into our country to harm us versus those that come in for an intent to get a job, support a family. The entry is still illegal. We have a responsibility to enforce the law in all respects, but we still have to recognize a distinction there.

Secondly, as you indicated, the pull, the magnet that brings in those that are coming in for job purposes or other purposes into this country really diverts our resources, consumes our resources, as compared to focusing on those that are coming in to harm us. So the temporary worker enhances security, gives a legal path, and it really mirrors what we did last week with two announcements, which was to reward those that are seeking a legal means to come to this country and to deter and discourage those that are trying to come in illegally. So I think the temporary worker program does that. It discourages illegal flow, and thereby it enhances security.

Mr. HAMILTON. Senator, may I just add—I know you didn't direct the question to us, but it raises a point that is very important to the Commission and that is the tie between border security and immigration. I think what we are trying to say in our report is that that is an enormously important tie. You cannot put those two things in separate boxes and deal with immigration over here and border security over here.

We believe you have got to have a biometric entry/exit system that is comprehensive. People come into this country all sorts of ways, not just across the border in Texas. They come across there in great numbers, but many, many ways they get into this country, and we have got to have a system that is comprehensive enough to deal with all of these people coming in.

Almost all of them come in with very benign purposes. We want them to come in, but we have got to be able to sort them out. We think officials have to have access to files on the visitors and the immigrants that are coming into this country so that they can make a judgment and make it quickly, as they often have to do.

We think you have to have an exchange of information on these people with other countries because most of them come from other countries, I guess by definition. Real-time verification of passports—we cannot do that today, but we have to try to do it and work toward that. And we see, of course, a growing role for partnership with State and local officials because the Federal Government simply is not going to be able to do it all. Part of all of this is secure identification of U.S. citizens, as well.

So we see this as an enormously important part of the national security of the United States. These people got into this country all sorts of ways. They cooperated with corrupt officials. They used fraud. They lied. They worked with human traffickers to get into the country. We have got to be able to identify these people. We have got to get the information on it, and once we get the information on it, we have got to put it into a center where it can be accessible to everybody.

And beyond intelligence, somebody has to be in charge to take charge of the case, to manage the case, which was not done on 9/11. Nobody was in charge, nobody managed it. When we learned about these fellows out in San Diego, we had bits and pieces of information about them and nobody put it all together.

George Tenet was asked by us—when he learned in August of 2000 about Moussaoui in Minneapolis and we asked him what did he do about it. He said, well, I put some of my CIA people to work with the FBI. And we pushed him a little harder on it and he said this was the FBI's case.

Now, I don't think his answer was wrong, but it just illustrates what happened prior to 9/11. Nobody took charge of the case, nobody managed the case, and that is what we are trying to correct with our proposal on the national counterterrorism center. You have got to have somebody not only that collects the information, but once the information is collected, somebody has to manage it and say I am taking charge of this.

Chairman HATCH. Thank you.

Senator Kennedy.

Senator KENNEDY. Thank you very much, and I thank our panelists for remarkable public service. We can tell from listening to Lee Hamilton how strongly he feels about this undertaking, and I know it is a feeling that is shared by all of you.

Right here is a book of hearings and it is hearings that I held in 1971 about what has happened to other presidential commissions, and the fact was nothing, nothing; they are all gathering dust. These were the Scranton Commission on Campus Unrest, Katzenbach on Crime, Eisenhower on the Causes of Violence, Hesburgh on Civil Rights, many others on health and the list goes on. That isn't what is going to happen to this, but it is an important historical fact about what the history has been. That is why I think there is a sense of urgency about taking action at this time.

Let me go to a very important part of the recommendations that were mentioned by your joint statement, and also Asa Hutchinson, in the jurisdiction of this Committee and that is the sections on privacy and civil liberties. You make the very important point that the new focus on collecting and sharing more and more information about people raises these serious concerns.

You say that no one in Government is now responsible for making sure that everything that is done in the name of fighting terrorism is done consistently with the historic and essential commitment to personal privacy and liberty. You recommend that an office be established to handle this issue government-wide. Both of you have generous comments about it in your testimony.

I would like to just sort of ask rhetorical questions and you will get the thrust of it. I am interested about how serious the Commission was in making these recommendations and whether all of you will put the full weight of credibility behind it and make it clear that this office, to be effective, needs adequate resources and access and clout if it is going to be able to be effective in doing what you have outlined would be so important to be done.

In the 9/11 Commission report, it talks about the possibility of setting up a panel similar to the Foreign Intelligence Advisory Board. I am interested in, one, the kind of commitment that all of you feel we should have on this, how important it is, and then whether this ought to be an internal or external board. Should it be just left to the particular agency or should it be a panel that is established within the Government, or should it be established inside the Government and one that would be outside but working like the Foreign Intelligence Advisory Board?

Mr. HAMILTON. Well, Senator, we are very serious about it. Look, in order to get at the terrorists, you put into place a lot of things that are intrusive on the lives of Americans. We encounter it every-

day. We have become more tolerant of those intrusions because of our fear, because of our concern about the terrorists.

But everywhere you turn, including in our report, you keep stacking up restrictions on Americans and you expand the powers of Government in the FBI, in the DHS and a lot of other places. Now, that has to be a concern to everybody and we didn't know exactly how to deal with that, but one of the things that struck us was that there was not in the Government any single place across departments, across agencies that looked at the questions of privacy and civil liberties.

I heard—I have it in mind; I know it is highly classified. I can't talk about it, except to say it is an astounding intrusion into the lives of ordinary Americans that is routine today in Government. Now, a lot of this stuff is highly classified, and so I am very committed to the idea of a board. And you asked what resources, what power should it have. It ought to have adequate resources. It ought to have a very tough investigative staff and it ought to be a very active board and agency, and it has to be able to cut across all departments. I don't know how you set that up, except you set it up through the President and the White House.

Mr. GORTON. Senator Kennedy, I remember very distinctly that this subject came up in the initial organizing meeting of the 9/11 Commission, and it flowed through from the first day to the last. It informs our general statement that as the Congress or administration considers new powers that it has got to weigh what the goal of the exercise of those new powers is against what the effect of those new powers will be on individual citizens within the United States. It informs the recommendation that we make with respect to this board, this agency, this individual, whose sole responsibility it will be to see to the civil rights of all Americans.

One of the decisions we tried to make—it has been very difficult, I can tell you, in the four weeks of making speeches on this subject. Everyone wants to know, well, what is your most important recommendation? How would you rank them one through five?

We tried to avoid that. We think that they are all of great importance and we think that this one, or the connection of these two or three are of great importance as we fight terrorism in the United States.

Senator KENNEDY. Well, that is powerful support.

Secretary Hutchinson, border security, entry-exit—we have talked about that here. This has been talked about since the Hesburgh Commission on Immigration going back 25 years. We passed a border security bill. We are doing reasonably well in terms of the entry, but not very well in terms of the exit. There have been some estimates that in order to have a really effective system, it is going to take 7, 8, 9 years.

Last year, for example, we had actually a reduction in requests by the administration in terms of border security, somewhere around $300 million and it was reduced by over $100 million, and efforts were made in a bipartisan way to restore it.

Let me ask you about the exit aspects just briefly, when you think that can be effective so that we have comprehensive entry and exit, just as quickly as we can because there is one other area I want to cover.

Mr. HUTCHINSON. We have an exit capability that is limited to biographical information at present, and so we do have information that comes in from our airline departure information so that we can see when people leave our land borders as well. We need to add the biometric feature to it, which we are testing at about 15 airports now. We will get the right technology, and then we move to our land borders. This is an enormously challenging prospect and funding is a part of it. We can go back and forth on that, but the administration did request $400 million in 1904.

Senator KENNEDY. Ms. Baginski, on the watch list, I want to know—and my time is running out here—about how this works for the average person. Let me give you an example. I got on the watch list last April. I was taking a plane to Boston and I got out to U.S. Air and I came up at quarter seven and I wanted my ticket. They said we can't give it to you. I said, well, wait a minute, here is a visa; there must have been a mix-up. And the person behind the gate said I can't sell it to you; you can't buy a ticket to go on the airline to Boston.

I said, well, why not? We can't tell you. Well, I said let me talk to the supervisor on that. This is at five of seven. The plane is about to leave, and finally the supervisor said okay. I thought it was a mix-up in my office, which it wasn't. I got to Boston and I said there has been a mix-up on this thing in Boston. What in the world has happened?

I tried to get on the plane back to Washington. You can't get on the plane. I went up to the desk and I said I have been getting on this plane for 42 years and why can't I get on the plane back to Washington. They said you can't get on the plane back to Washington. So my administrative assistant talked to the Department of Homeland Security and they said there was some mistake. It happened three more times, and finally Secretary Ridge called to apologize on it. It happened even after he called to apologize because my name was on the list at the airports and with the airlines, and Homeland Security couldn't get my name off the list for a period of weeks.

Now, if they have that kind of difficulty with a member of Congress—my office has a number of instances where we have the leader of a distinguished medical school in New England, and the list goes on—how in the world are average Americans who are going to get caught up in this kind of thing going to be able to get to be treated fairly and not have their rights abused?

Then just finally if you can just tell us what the justification was for the investigation of those FBI agents out in Colorado with the six agents interviewing that 21-year-old woman that has been reported in the paper.

Thank you.

Ms. BAGINSKI. I will deal with the last issue first because I think I can deal with that more succinctly. We have read the New York Times representation of our activities and compared that to the actual activities. I think as you know, we engaged in interviews of people based on specific intelligence that they planned to perpetrate violent acts at the Democratic National Convention, and we are also looking at the Republican National Convention in that dimension.

There are many of you who I think are rightly concerned about that in light of the press treatment. What we have offered to other committees and what we would like to offer to you is a written accounting step by step of what was done so we can separate fact from fiction on this and hopefully ease your concerns and those of the American people.

Chairman HATCH. We would appreciate that.

Senator LEAHY. I would like one, too.

Ms. BAGINSKI. Yes, sir. On the issue of the—

Chairman HATCH. How about the conspiracy to stop Senator Kennedy from getting where he wants to go?

[Laughter.]

Senator KENNEDY. Notice that I didn't accuse the Republicans of doing that.

Chairman HATCH. No, no, but it was implied, we know.

[Laughter.]

Ms. BAGINSKI. I think actually the answer to that is a combination of the two of us.

Asa, do you want to start?

Mr. HUTCHINSON. If I might, Senator, we do regret that inconvenience to you.

Senator KENNEDY. No problem, no problem.

Chairman HATCH. Asa, don't be so quick to say that.

[Laughter.]

Senator LEAHY. We have had this problem with Irish terrorists before.

Mr. HUTCHINSON. It is important for the average citizen to know the process. They can call our TSA ombudsman, who will take the information down, verify that their name is not the same as what is confusingly similar on the list. And we can actually enter into the database that they have been cleared, so that that should be prevented in the future. So there is a process to clear names, but it does illustrate the importance of improving the whole system, which we are very aggressively working to do. We need to own that no-fly list.

Thank you very much, Mr. Chairman.

Senator KENNEDY. My time is up. Thank you, Mr. Chairman.

Chairman HATCH. Ms. Baginski?

Ms. BAGINSKI. Just to complete the part of it in terms of the responsibility for the authoritative list, of course, on the international side it resides with the TTIC, the Terrorist Threat Integration Center, so the vetting of those names. And then, of course, for the domestic side, it would come from the FBI. And those are fused, I think, as you know, in the Terrorist Screening Center. So I do have some responsibility for the pedigree of that information that comes from intelligence, and I want to assure you that we review that on a regular basis.

Chairman HATCH. Thank you.

Senator DeWine.

Senator DEWINE. Thank you, Mr. Chairman. Let me thank all of you for your great work and the very wonderful job each one of you has done.

Ms. Baginski, let me ask you the first question. You talked about in great detail improvement in the area of intelligence and infor-

mation. The September 11th Commission outlined in great detail a lot of the problems, and I think we all are very familiar with the story leading up to September 11th.

Explain to me in layman's terms what is different today from what was the situation on September 10th as far as the FBI is concerned, and in terms of an FBI agent. Senator Leahy has described the problem and our continuing frustration, and I know Director Mueller has the same frustration with the computer system that is not progressing as fast as we would like it to.

What is the difference today for an agent who seeks information or who needs information or who wants to share information, and not in general terms, but in real specific terms?

Ms. BAGINSKI. I can answer this in terms of technology and also—

Senator DEWINE. No, I don't want that. Give me an example that I can understand. What matters? What is the difference today?

Ms. BAGINSKI. I think there are three areas and I will try to cover them in as much detail as I can. First—

Senator DEWINE. No, no, I don't want three areas.

Ms. BAGINSKI. You want a specific example?

Senator DEWINE. Yes. Give me an example; tell me a story in the next 5 minutes. What difference does it make? How are we any better off today than we were prior to September 11th? Tell the American people why they should feel better.

Ms. BAGINSKI. On the first order, terrorism is the number one priority of every member of the FBI. Since 9/11, as you know, with our responsibility, we have expanded our number of joint terrorism task forces, which are—

Senator DEWINE. Excuse me. I am sorry.

Ms. BAGINSKI. I am still not doing what you want. I know you want a specific example.

Senator DEWINE. Okay, no. Tell me what an FBI agent knows today or can do today that he or she couldn't do.

Ms. BAGINSKI. Okay.

Senator DEWINE. What can they share? What comes up on their computer screen? How is that?

Ms. BAGINSKI. I got it. Before 9/11, agents could not send with any ease e-mails to one another across a secret network. Now, that can be done. Before 9/11, agents did not have access to other agency intelligence production in the joint terrorism task forces, and now they do. So they can actually go into a database and enter on that like system and actually access that information and find out if there is other information that they need and can act upon in terms of working the case.

Prior to 9/11, all cases in the FBI, I think as you have all said, would have been opened first as counterterrorism cases in the sense of prosecution. Post 9/11, all cases in the counterterrorism arena are opened as intelligence cases first, so that instead of the intelligence component being a sub-file in the larger case, the intelligence is driving that and is one of the tools in the tool kit that the agent brings to bear on neutralizing a threat.

Prior to 9/11, the intelligence analysts at the FBI could not with any ease ask questions of data that was aggregated for them and do federated queries across the database. Since 9/11, we can.

Senator DEWINE. What kind of search can I do now?

Ms. BAGINSKI. If you are an analyst, you can do a search against a finite body of information at the secret level on one network and at the top secret and higher on another network that, in fact, is exactly what you can do in your living room. You can ask questions of the data and the answers will be pushed to you.

Senator DEWINE. What if I am an agent in San Diego and I am working on a particular case and I am wondering if there is a similar case somewhere else in the country and I want to put in a series of words? Can I do that?

Ms. BAGINSKI. You can. You can do a word search and you will get the answer.

Senator DEWINE. I will now get the answer?

Ms. BAGINSKI. Yes, sir.

Senator DEWINE. What can't I do now that I should be able to do in 2 years or 3 years or 4 years? What are you frustrated about? What are you upset about? What bothers you today that you can't do?

Ms. BAGINSKI. I think there are three critical areas. The first would be being able to operate in a top-secret, code-word environment, which is connected to the Commission's recommendation to help us with our secure, classified information facilities.

All of the field offices have secure, classified information facilities. They are very, very small areas. I sometimes joke that they look like closets, and they generally have an Intelink computer there. What I am saying is if we want to be part of this network in which the larger intelligence community operates, we need that kind of—

Senator DEWINE. Excuse me. I don't understand what that means. Does that mean that only a limited number of agents have access to that? Is that the problem, or what does that mean?

Ms. BAGINSKI. Well, the physical access is determined by your security clearance. So, of course, everyone that is cleared to the secret and top secret area, which is the way that we do our clearances, would have access. My point is it is usually one or two terminals which—it is the hardware that is limiting, if you understand. The secured, classified information space is necessary to be expanded to accommodate that hardware and the network.

Senator DEWINE. So that creates the problem of what, just not enough people being able to get at it that need to get at it?

Ms. BAGINSKI. Yes, sir. As I expand the number of analysts that are out in the field, which is what I really need to do, I am going to need more space for them to access that classified information.

Senator DEWINE. Would every field office have access to it, though?

Ms. BAGINSKI. Yes, sir.

Senator DEWINE. What other problems are you having that you would be able to solve in the next couple of years when the system is totally up?

Ms. BAGINSKI. The other, I think, issue for all of us is what I think Senator Leahy was referring to, which is the automatic entry of information into corporate databases. Trilogy, as you know, was three initiatives. Hardware is there; the LANs are there. It is the application, the virtual case file case management application, that

allows the automatic entry of this information into corporate databases for follow-on analysis. That is the part that is delayed. So we have delivered two, except for this application.

I think the solution of that in the hands of our chief information officer will help the robustness of my analysts' database, which is called the Investigative Data Warehouse. That will help my analysts have the breadth they need of information to actually do the queries against.

Senator DEWINE. When do you expect that to be up?

Ms. BAGINSKI. We will have some delivery of that by the end of this year, and I would like to get back to you with a specific date because I am actually not as current on that as I should be.

Senator DEWINE. Sure.

Ms. BAGINSKI. Lastly, for me, I have a training issue and it is not a small issue and it is going to require an investment both in terms of facilities and in terms of expertise and in terms of time.

In building this cadre that has been recommended to us by the Commission, and I think very rightly recommended by the Commission, there is a wonderful training capacity in Quantico. There is a very powerful FBI, and I would say law enforcement brand in Quantico, but to build in there that same expertise and capacity for teaching intelligence to the agents and to the analysts and to the linguists, and then to our partners in State and local law enforcement—that actually is an investment and is going to be both in time and in some facilities and infrastructure.

I am very pleased with the work we have done. I just want to share with you very briefly—we have just overhauled our basic analysis training, seven core learning objectives. Those learning objectives are now being worked into the new agent's class. They are the same learning objectives, the same modules, and the magic will be that we will have agents and analysts doing joint exercises together when they are in training. Now, we need to offer that to our State and local partners. The National Academy has been very powerful in that partnership. We need to be able to offer that same thing.

Thank you.

Senator DEWINE. Thank you very much. I appreciate it.

Chairman HATCH. Senator Leahy wanted to interject here.

Senator LEAHY. I am not sure I fully understood. To follow what Senator DeWine was saying, and I am not sure I understood the question, if you want to do a search, for example, could you put a series of words in the same search, like, for example, southwestern, alien, flight training? Could you put that all in as one thing and have it searched down there, or do you have to put in each word separately in the search?

Ms. BAGINSKI. We can, in fact, in the Investigative Data Warehouse, which actually started out as something called the Secure Operational Prototype—it was all based on terrorism—we can do the string that you are talking about, the multiple words.

Senator LEAHY. And you can do that in—

Ms. BAGINSKI. I beg your pardon?

Senator LEAHY. You can do that in—

Ms. BAGINSKI. In Trilogy? Is that what you mean, sir?

Senator LEAHY. Trilogy, yes.

Ms. BAGINSKI. IDW is actually something that I would call separate from the Trilogy package that you and I have been talking about.

Senator LEAHY. You can do it in Trilogy, though?

Ms. BAGINSKI. Trilogy is not a data warehouse that you would search against. That is why I am having trouble answering the question. Trilogy is hardware, as you pointed out, computers on desktops. It is local area networks, wide area networks for the connectivity, and it is the case management application.

The case management application then feeds the Integrated Data Warehouse that I am describing that allows me to do the search.

Senator LEAHY. You could do a multi-word search?

Ms. BAGINSKI. In the Integrated Data Warehouse, yes, sir.

Senator LEAHY. Thank you.

Chairman HATCH. Senator Kohl.

Senator KOHL. Thank you, Mr. Chairman.

We appreciate very much your appearance here this morning. I have three questions that I would like to address to the Commission members, and I think all of us here and people who are watching on television are interested in your opinions on these questions because you have been so immersed and you have a written a report which is on the bestseller list. So, obviously, all Americans are concerned with your work and with what is going to happen to your work.

As Senator Kennedy pointed out, the history of commissions in terms of their effectiveness and implementation of their recommendations is not good. In the case of the world in which we are living right now, your recommendations are high on the list of every American's thoughts.

So, first of all, on your arguably most important recommendation that we have a national intelligence director to coordinate all the things that we are talking about this morning and the things that you have recommended in your report, already we have seen that the Secretary of Defense has basically come to a disagreement with you on the need for a national intelligence director or on the efficacy of such a person. The President himself, I believe, has said perhaps a NID, a director, but not with control over budgets and personnel.

Now, the way Washington works is if the Secretary of Defense, who spends 80 percent of the intelligence money that we allocate, and the President are not in support of that recommendation, what are the chances of getting that through, number one?

Number two, this is all about fighting terrorism and making Americans more secure. In the Muslim world today, our standing is as low as it has ever been. The number of people who are in strong dislike, if not outright hatred, of the United States and willing to do as much damage as they can to the United States—the number of people in that category is growing ever higher everyday. How are we going to ever win the fight on terrorism and make America more secure if, in the short term, if not the long term, we are not making progress in this area?

Number three, I would like to ask you about the color coding system. Does it make any sense, in your opinion, for us to have a national color coding system; for example, the orange, which is the

second highest alert, to place the whole country on an orange alert, when, in all probability, it is specific parts of our country that need to be placed on alert? Do we need to sharpen up that color coding system to make Americans all across our country more aware of who is at the greatest risk and who is at minimum risk when, in fact, we issue that kind of a warning to the American people?

So it is three things—the national intelligence director, our problems within the Muslim world today and how are they going to manifest themselves going forward, and the color coding alert system.

Mr. GORTON. You have covered the waterfront, Senator Kohl.

Senator KOHL. Well, you have been thinking about this now for months and months and months, and you obviously have opinions that are of great interest to those who are watching on television.

Mr. GORTON. First, on the national intelligence director, on that system, remember we pair two things—the national counterterrorism center that we think is vital and we have discussed earlier, whose functions are just counterterrorism, and a national intelligence director, who will cover the waterfront as far as intelligence is concerned.

In one sense, ours is a very conservative recommendation because we go back with this National intelligence director to what the CIA Director was supposed to have been in 1947 when it was created, which was the overseer of all of the intelligence of the United States.

Well, first, of course, the CIA has become bigger and more complicated. Just running the CIA is clearly a full-time job. But, secondly, because of the absence of any effective budget control over roughly 80 percent of the budget, no CIA Director could really fulfill that function in any event.

So what we think is that 50 years ought to have taught us that if you are going to have someone who oversees all of the intelligence activities of the United States and does planning for all of them, that individual should have control over at least the supervision of the budget and some very real influence over personnel, as well. And we do feel very strongly about that. If you just do again what you did in 1947, you aren't going to have any more effect. That position must have power.

I guess personally I am less pessimistic than you are. I think the administration's objections to it at least are softening, but it is going to be a decision Congress is going to have to make. And we feel very, very strongly that if you are going to create a national intelligence director, that individual should have budget authority and should have some personnel authority.

Certainly, no national intelligence director is going to starve the military of the intelligence information that it needs. It is impossible to imagine.

Second, we make recommendations with respect to the war on terrorism on three levels, and we distinguish those levels. One is that in dealing with those enemies that are absolutely irreconcilable, you know, we simply have to recognize they declared war on us a long time ago, and we are at war with them, and it should be conducted as a war, and we need to deny them sanctuaries and the like. The overwhelming challenge is the one that you raise, is

how do you separate that large but small in percentage group of enemies from the vast majority of Muslims who are peace loving and want better lives for themselves and for their children. That is a tremendous foreign policy challenge, but it is a challenge that we must make. We make some general suggestions in that connection, more specific with three countries, but general suggestions about carrying out our own message.

Finally, on the color code system, I share your frustration. Just to tell everyone in the United States you are on orange alert now, that makes it even harder to get into an airport or on an airplane, but does not tell any local enforcement that there is some specific challenge in your place, seems to me at least to be rather frustrating.

I think the more recent one, where the warnings were very specific, is the way in which we should go. Now, there is still going to be criticisms as there have been of that, but I do think that at least those are meaningful.

Now, the real paradox in this country today is that we have not had any other attack since 9/11, and every time there is not one, people become more relaxed, and to a certain extent more complacent. Even if a warning from Homeland Security may have prevented an attack, we will never know that it did, and it leads to a certain degree of cynicism with respect to whether or not we were calling "wolf." That is a challenge. It is a challenge any administration will have. But I do think the more specific way in which the Department is operating is better than that national orange alert.

Mr. HUTCHINSON. Senator Kohl, could I just jump in there? That we certainly share the reservation about raising the threat level nationally if we have intelligence that we can narrow it. We are very grateful that the intelligence collection was very effective this last time. We were able to do it narrow in the financial sector in certain geographic areas, so we recognize, and we do evaluate the burden that falls nationally with the law enforcement community when we do raise that threat level, and we are certainly looking, with Congress, for ways to refine that system.

Senator KOHL. Congressman Hamilton, would you—

Mr. HAMILTON. Senator Kohl, first of all, I have been getting an inferiority complex here, hearing all these stories about ineffective presidential commissions and Congressional commissions. I want to respond to that, and say that there are some commissions that have worked. The Greenspan Commission on Social Security reported. The Congress adopted it in total, a few months before the election, as I recall. I served on the Hart-Rudman Commission. This gentleman would not be sitting here today if it had not been for our recommendations. We recommended the Department of Homeland Security. So some of these commissions do have recommendations adopted.

You asked what are the changes of the National Intelligence

Director and the National Counterterrorism Center being adopted. That is a tough one. Look, we understand we have put forward here a fairly radical proposal. The President has endorsed the idea of a National Intelligence Director. He has endorsed the idea of a National Center for Counterterrorism. What is not clear is what

powers he would give to those positions, and I think that is still a matter very much under discussion in the administration.

Secretary Rumsfeld expressed a wariness. He did not object to a National Intelligence Director. He just expressed a kind of a wariness about the idea. That is understandable.

Look, we have a tough problem here. On the one hand the military says, we want all of this intelligence to protect the war-maker, and I do not know anybody that wants to make it more difficult for the war-maker. We want to provide information for the war-maker, and none of us want to limit the intelligence flowing to the war-maker. But you also have an obligation to protect the American people. In order to protect the American people, you have to have intelligence not just flowing to the war-maker, you have to have intelligence flowing to this policymaker, the strategic and the national intelligence.

Where do you draw the line between strategic and national intelligence on the one hand, tactical intelligence on the other hand? In many cases it is very easy, very simple. But there are a number of areas, particularly in the areas in which the Defense Intelligence Agency is involved, for example, where it gets a little murky, and the Secretary is right to be concerned about that. Take the U–2. The U–2 flies all over the place, takes a lot of pictures, and many of those pictures are of enormous importance to the tactical commander on the field. Nobody wants to interrupt that. But that U–2 also takes pictures that are tremendously important to the policymaker. Who should control that asset?

What I am suggesting here is that the debate that is going on is not a frivolous one. It is not an ideological one. It is a very practical one, and the issues are not always clear-cut. They often are. So I have welcomed the support that has been shown to the Commission's recommendations. I understand a lot of recommendations we made raise big questions in the FBI, big questions at the DHS, and certainly big questions at the DOD. I think we can work through this and come up with a solution that is reasonably satisfactory.

The second question about the Muslim world, Senator Gorton I think was on the mark there. The distinction that has to be made is this very, very small group of people who are out to kill us, al Qaeda, Osama bin Laden and his top cohorts. That is not a hard question from a foreign policy point of view. You have got to remove them, whatever that means, capture, kill, whatever. You are not going to convert Osama bin Laden to democracy or to our way of life. In a sense, that is easier—not easy to carry out, but easy to articulate—foreign policy. The tough part is this Muslim world that you express your concern about, and so do we in the report.

Here you have, stretching from North Africa to Indonesia, millions and billions of people who, if the polls are correct, do not think very highly of us, hold us in very low esteem, admire Osama bin Laden, are sympathetic with much of what he says, but may not endorse his violence. And if the war on terrorism is to be won, we have to appeal to those people, and that is one of the reasons we say this is a generational challenge. You cannot do it in a year or two.

How do you do it? Well, we tried to put forward some suggestions, but the important point here is, for me at least, is if you are thinking about counterterrorism policy, what should the United States do to deal with terrorism? You cannot get all hung up in the boxes. You cannot get hung up on terrorist financing. You cannot get hung up on the FBI. You cannot get hung up on DHS. You have to see it as necessary to put together a integrated, balanced effort dealing with military action, covert action, law enforcement, treasury actions to stop the flow of money, public diplomacy in many, many areas. The tough part of counterterrorism policy is to get all of that integrated and balanced.

One of the aspects of it is to show to them, the Muslim world, if you want to put it in simple terms, that we are on their side in terms of wanting a better life. We want for them a better life and better opportunities. You know the figures with regard to young men in these countries, 40, 50 percent unemployment. Where do they go? What do they do? Why do they turn to violence? That is not a impossible question to answer. Their life has nothing in it to give them any hope. We cannot solve all those problems. We do not have the resources to solve all those problems. We can encourage the governments to move in the right direction, become more open, more transparent, to become more concerned about their people. We think there are a lot of things you can do to that are perhaps symbolic, but nonetheless important. Every politician knows how important it is to let people know you are on their side. You have constituents that come up to you all the time that ask you to do something that you cannot possibly do. But the important thing, in a political sense, is to let those people know you are on their side, you want to help them with their problem. Maybe I am too simplistic about this, but I think that is what you have to do in American foreign policy, you have to let these people know we are on their side and we want to help.

Okay. You have decided to put $100 million, I think it is—I may not be quite right on that figure—into the school system in Pakistan. If you know anything about the school system in Pakistan, that is a drop in the bucket, but I think it is very, very important to let those people know we want a decent education for a lot of Pakistanis, and we want to provide an agenda of hope, and we want to be on the side of hope for these people.

What does Osama bin Laden offer these people? Death, a very tough life. What do we offer? We have an awful lot to offer, and we have just got to be able to put this all together in American foreign policy in terms of a robust public diplomacy, in terms of increased scholarships.

I used to go to Eastern Europe all the time when we had those cultural centers during the Cold War, and people were constantly attacking them as being a waste of money and a waste of time, but you would visit those offices in Prague or Warsaw at 10 o'clock at night, and we had to throw then out of there. They were so anxious to learn something about the United States of America, and I thought those were enormously important, and I think you have to do a lot more of the same with regard to this Muslim world.

We are not going to solve this problem in a week or two or a year or two or in my lifetime, but we have to get started on it.

Chairman HATCH. Thank you, Lee.

Senator Chambliss.

Senator CHAMBLISS. Thank you, Mr. Chairman.

A very profound statement, Lee. I am one of the folks who was somewhat skeptical about the formation of this Commission when it started, in some part because of exactly what Senator Kennedy alluded to there, that thick book he held up. I know he is exactly right about it, but I just want to tell you guys, and I have known both of you for a decade and have had the opportunity to work with you and have great respect for both of you, and I think your Commission did a really find job, not just in what you recommended, but you did an awful lot of research and you put it in black and white where Americans can understand it. I hope this report continues to be on the best seller list for months to come.

I appreciate you setting the record straight relative to what the President and Secretary Rumsfeld, as well as others in the administration, have said. I am one who, because of your report in part, has come around to a way of thinking that we do need a National Intelligence Director, and we are going to have one. It may take us somewhat longer than what some folks would like for it to happen, but it is going to happen. But the President has been very specific in saying that he has not shut the door on what kind of power and authority this individual ought to have and that is open for discussion. That is the kind of leadership that we expect out of our President and we are getting out of our President on this specific issue.

There has been a compilation, Mr. Chairman, of a side-by-side of the 41 recommendations that the 9/11 Commission made, and either the action on the part of the administration, a lot of which was alluded to by Secretary Hutchinson, and the ones that have not been acted on, the particular consideration that is being given to those recommendations. Thirty-nine of the 41 have either been directly acted on or are under consideration. The only two that have not been, interestingly enough, are the two relative to the reorganization of Congress.

[Laughter.]

Senator CHAMBLISS. I introduced a copy of that yesterday in the Intelligence Committee hearing, and I would like unanimous consent to introduce that today as part of this hearing.

Chairman HATCH. Without objection.

Senator CHAMBLISS. Ms. Baginski, I want to tell you an anecdote particularly with the strong support coming from the 9/11 Commission about the PATRIOT Act. I have been a strong supporter of it. I think it was the right thing for us to do, and I think it has been very effective. I met with most of my JTTF in Atlanta recently, and an interesting comment came out of that group when we were talking about the PATRIOT Act. What one FBI agent said was, he said: The enactment of the PATRIOT Act has been crucial to us winning the war on terrorism, and we need for every bit of it to be extended. And he said: I will tell you that it has not been the great asset that a lot of people thought it would be relative to the arrest and prosecution of terrorists, but what it has allowed us more importantly to do, and on many more cases than have been prosecuted, is to eliminate suspects from suspected acts of terrorism.

VerDate Aug 31 2005 15:22 Oct 22, 2008 Jkt 096459 PO 00000 Frm 00040 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\96459.TXT SJUD1 PsN: CMORC

I think that is critically important when we are talking about invasion of freedom and liberty, and, Lee, you are right, we have a delicate balance there that the PATRIOT Act has to meet. But I was particularly intrigued when that agent told me that we have relieved a lot of people's minds because we had the PATRIOT Act. We would not have been able to do the that had we not had the PATRIOT Act.

One quick question, Lee and Slade. You are, rightly I think, very critical of the FBI from an information sharing standpoint. You identified them as one of the biggest abusers of the frankly lack of information sharing, and I have done the same thing, as you know. While there have been great strides made there, the one glaring area to me you left out was DOD's information sharing. What did you conclude relative to the acts of DOD regarding information sharing, and is there any kind of model there that we can look at for the future?

Mr. HAMILTON. There are a number of very important intelligence collection agencies in DOD. You have got the NSA, you have got the NGA, you have got the NRO, and you have got the Defense Intelligence Agency. There are probably others as well. And one of the interesting things about the intelligence community is that, as you know, that is the way it is organized. It is organized around collection, how you collect. And when you stop to think about it, it ought to be, at least in my mind, not organized on the way you collect, but it ought to be organized on your mission, what you are trying to accomplish, and that is why we get into the national intelligence centers and the National Counterterrorism Center.

We believe all of those agencies I have mentioned and others do a very good job of collecting information. We collect vast amounts of information in this Government. Every minute or two we are collecting millions of bytes of data, and the big problem is not so much collection as it is analysis and assessment. But we think the stovepipe phenomenon has seriously hurt our overall intelligence agency, and I think there have been improvements made since 9/11, but nonetheless, still there is this kind of focus on, we collected this information, we will keep it, and the sharing mechanisms are informal, they are not institutionalized. They are better I think than they were, but I think we have a long way to go to get the kind of free flow of information that is vital to counterterrorism efforts.

Mr. GORTON. Lee is entirely right in that connection, and Senator Kennedy referred to the fact that much of the information that we gather through the signals things does not get translated or does not get translated in real time, and the sharing arrangements were highly informal. Now, one major improvement since 9/11 was the creation of the Terrorist Threat Integration Center, which is designed to see to it that information from here and information from there and from the CIA and the Defense Department gets to someone who can distribute it to the people in the agencies who know about it. In one very real sense, our recommendation for a National Counterterrorism Center builds on that. Our impression is that it has done a pretty good job, but it is headed by a relatively mid-level executive on loan from the CIA, and it has people on loan

from the FBI and on loan from the Defense Department and other agencies, who know their long-term career is somewhere else. They obviously cannot tell those agencies what to do.

If you have a National Counterterrorism Center headed by a presidential appointee confirmed by the Senate with the power to demand cooperation, and even more significantly, the power to say: here is something we are missing in the field of terrorism, I think it falls within the FBI's jurisdiction, so you go out and look for it here, CIA go out and look for it somewhere else, we will make that a much more powerful and effective entity.

Are we doing a better job now than we were before 9/11? There is no question about it. Can we do a better job, including the integration of these Defense Department agencies which are really the 800-pound gorilla? At least from the point of view of the technology they have and the money they have, clearly we can.

Senator CHAMBLISS. Thank you, and thanks to all of you for the great job you are doing.

Chairman HATCH. Thank you, Senator.

Senator Feingold.

Senator FEINGOLD. Thank you, Mr. Chairman for holding this hearing.

I too want to thank Commissioners Hamilton and Gorton, and all the Commissioners and members of the staff of the 9/11 Commission for your incredibly important and effective service. I cannot emphasize enough how vital your work is to the American people, and how significant and refreshing it is, that your reports and recommendations are bipartisan and unanimous.

Chairman Hamilton, let me particularly thank you for your comments today, your candor with regard to certain, as you described them, astonishing powers of the Government, and also your enormous eloquence in your recent comments to Senator Kohl about some of the real foreign policy challenges that are before us.

I supported the creation of the 9/11 Commission because I believed it was crucial to review what went wrong leading up to the fateful day in September, 3 years ago, what we can learn from those mistakes and what we should do to improve our Nation's defenses against a future attack. But I will confess that this product greatly exceeded my expectations and even my hopes. You have provided us with a template for how to make our country safer and stronger. It is not time to implement these recommendations. We need to work out the details carefully but quickly, and in a bipartisan manner, taking our cue from the work of the Commission. Our Nation must effectively combat the terrorist threat we face. That must be the very highest priority of the Congress. We need real reforms now, particularly with regard to our intelligence community and our intelligence oversight, and I obviously look forward to working with my colleagues on both sides of the aisle as we do that.

Let me ask questions of Congressman Hamilton and Senator Gorton. The Commission has created an extraordinary sense of urgency about its recommendations. It seems very possible, if not likely, that we will consider the legislation on the floor with regard to this prior to the election. You have created a very fast-moving train for these recommendations, and I do salute you for that. Both

of you served with distinction in the Congress, so you know very well that fast-moving legislative trains are vehicles that are tempting targets for pet projects. So I want to get your reaction to some possibilities that, given the highly-charged political atmosphere we are all working in, do not seem all that farfetched to me.

First let me ask you about potential efforts to attach or sneak in unrelated legislation to the bill that implements your recommendations. Will you as a bipartisan group oppose and speak out against efforts to use this legislation as a vehicle to force the enactment of other unrelated bills in the closing hours of this Congress? Congressman Hamilton.

Mr. HAMILTON. Senator, I do not think we view our responsibility to tell you how to get the job done. We think the recommendations we have made are important and we think they are urgent, and we urge quick action on them, but also careful action, as you said in your statement. The Commissioners are committed to trying to get the recommendations enacted, and we will speak out in favor of those recommendations. I understand, and Slade understands, the intricacies of the legislative process, but our eye will be on the target, and our target is to get these things enacted.

Mr. GORTON. Senator, we are not only gratified, but I may say, surprised at the quick and decisive action so far during the month of August, that 18 years in the Senate I do not remember an August when I was back here at hearings like this. It is an imposition on your time, and I think a tribute to your concern for what we have recommended that you have been doing this. And reading assiduously all our clips, I have not seen any indication of people trying to put pet projects on any of this legislation. We hope that you will pass legislation. Your procedures for doing so, of course, are for you to decide for yourself, and so I just simply associate myself with Lee. We hope you will act judiciously and carefully and thoughtfully, but because of the nature of this threat, we hope you will be able to act quickly.

Senator FEINGOLD. Thank you. I would just comment that the American people I think are proud of what you have done here, and one of the things that could most quickly undercut what you have done is if somehow this legislation became a vehicle for other agendas. But I do respect your caution in your answers.

In the report you repeatedly note the importance of protecting civil liberties, and I am pleased that you highlight that point, as I indicate, in your testimony as well. You say, Congressman Hamilton, that we must find ways of reconciling security with liberty, and of course, I strongly agree with you. Noting that some provisions of the PATRIOT Act will sunset at the end of 2005, you called for, and I am quoting here from page 394 of the report, "A full and informed debate on the PATRIOT Act." Can we count on you to speak out against attempts to short-circuit the full and informed debate you have called for by adding PATRIOT Act reauthorization provisions or new law enforcement powers to the legislation that we will potentially consider in the next few weeks?

Mr. HAMILTON. My recollection is that we commented with approval on the sunset provision in the PATRIOT Act, and because of the sensitivity of increasing Government powers, and the protection on the other hand of human freedom, human liberties, we

think it is a very, very important matter for the Congress to try to balance these as best they can. Your specific question, would we comment about any effort to short-circuit consideration of the PATRIOT Act, I think we recognize the issues in the PATRIOT Act are very serious issues, and we would favor full and open discussion of them.

Senator FEINGOLD. Senator Gorton.

Mr. GORTON. I cannot add to those comments. I agree with my Vice Chairman.

Senator FEINGOLD. In the few seconds I have left, let me simply say that it is almost inherently the case that if we were to completely reauthorize every word of the PATRIOT Act during this accelerated period between now and the election, that it is impossible for this Commission's recommendation with regard to this to occur, and that the proper time for that consideration is at the time of the expiration of the sunset, but I certainly am not trying to put words in your mouth, just I believe that is a reasonable conclusion from what the two of you have said.

Thank you, Mr. Chairman.

Chairman HATCH. Thank you, Senator.

Senator Schumer.

Senator SCHUMER. Thank you, Mr. Chairman. I thank you for having this hearing in a timely way.

And I thank all of our panelists for the good work they do. I have worked with Asa Hutchinson and Maureen Baginski in their respective roles, and they are both responsive and involved and really caring about tightening up security in our Nation. I cannot say enough good about the 9/11 Commission. I think it was just an incredible, an incredible, incredible tour de force in terms of the recommendations, in terms of the bipartisanship, in terms of the refusal to point fingers of blame, which makes the media all happy but does not really solve the problems here, but instead looks for the future. So I compliment you all on that.

I am worried. I want to address this to our two Commissioners. I know it has been touched on, but I am worried that a lot of your recommendations are either not going to happen or more likely, what usually happens in Washington, we look like we are doing something, but we do not do them. The Director of the National Intelligence is a classic. The President came out early for it, but did not give it the teeth, did not say he was for the budgetary and the hiring authority, which you had mentioned, Slade, was supposed to be in the original CIA and somehow got lost over the years. And then 2 days ago we heard Secretary Rumsfeld, and he is representing the Defense Department, and obviously, the interests of the Defense Department, come out and basically—I mean we all have been around Washington long enough to know he was throwing cold water on your proposals even if he did not say it directly.

So I have a few questions on that. First, are you going to take strong and direct action to try and make sure we enact a full DNI, Director of National Intelligence, with budgetary and hiring authority before Congress adjourns this year, including however you see fit to do it, making sure that the President supports those proposals or is told that he ought to? Slade?

Mr. GORTON. That is exactly what we have done. We have made our recommendations. We have said that our recommendations are integral, that they fit into one another, and that we cannot say that doing them partway or piecemeal is going to provide the necessary degree of public security for the people of the United States that it is our conclusion that they deserve and can have.

I think that all of us are probably more optimistic maybe than your question on this. We do not see, at least so far in any of the comments, some kind of veto coming from the administration, and we see that the legislation is going to be written here. Just 2 days ago, as I understand it, Senator Roberts and Senator Rockefeller submitted drafts to the Governmental Affairs Committee that are essentially what we have recommended. That is the legislation that we recommend be passed.

Senator SCHUMER. Right. Do you worry that the House may not, you may not get a vote on it in the House? The Senate you will get a vote on it one way or another.

Mr. GORTON. I think we will. I have already attended one House hearing in Los Angeles on the subject, and have another tomorrow. I think members of the House are equally interested in doing something.

Senator SCHUMER. Let me ask you this, because when Porter Goss was nominated, it was early on I think, I was the first Democrat to say good things about him. I think he is a good man. I served with him in the House, and I think he has integrity. My worry is that will be a substitute for doing the recommendations that you suggested on the Director of National Intelligence, that we will do Goss, and then we will say, Let us come back. Let us let him have an assessment. He has not been that friendly to your recommendations. What would you think of trying to tie the two together? I think this is much more of an issue of structure than of one individual person, but of us—and we could probably do this here in the Senate—saying, yes, let us approve Porter Goss, and let us approve the 9/11 Commission's recommendations on DNI at the same time?

Mr. GORTON. That is beyond our pay grade, Senator.

Senator SCHUMER. Oh, no, it is not. I would simply say to you that I am more worried maybe than you are. I was delighted to hear Pat Roberts come out and say what he did, but I think we have a long way to go, and frankly, that does not absolve this body. I think we have the same problems here, maybe even more so in terms of creating a Committee that has oversight over all intelligence with budgetary and other kinds of authority, which we do not have now, and no one is happy with the oversight that the Intelligence Committee is able to do because of their lack of power.

I would just hope that you will be real strong on this, saying it and then letting it—because if we do not do it by November, I am very worried we may never do it, and the fine work that you have done may be put on the bookshelf.

Do you have any comments on this, Lee?

Mr. HAMILTON. Well, we feel very positive about our recommendations. We think if they are adopted the country will be safer. We think it is terribly important that the National Intelligence Director have full authority of budget, information systems,

personnel, and we go so far as to say that if he does not have those powers, do not bother with it.

Senator SCHUMER. Right.

Mr. HAMILTON. No sense creating it because then you really are creating another layer of bureaucracy. We have been talking for 30 or 40 years around here about strengthening the power of the CIA Director, and we have done, you, and I in the past, have done some things that I think have been helpful, but he still is in a very anomalous position.

Senator SCHUMER. Will both of you and the Committee members have a running sort of—you will be commenting as we move through the process about this and that and the other, not just saying, these are our recommendations, we hope you do them, and then exiting the stage?

Mr. GORTON. No, we do not have any intention of exiting.

Senator SCHUMER. Great. That is good news.

Chairman HATCH. We have not seen you exit at all.

[Laughter.]

Chairman HATCH. We think you are hanging in there.

Senator SCHUMER. Do I have time for—

Chairman HATCH. You can have one more question.

Senator SCHUMER. Great, okay.

My next question relates to the issue of nuclear security. One of my great worries—and I think many of us share this, but particularly I have been focused on this—is that somebody slip a nuclear weapon into our country, and God forbid, explode it. I do not mean a dirty bomb. I mean a real nuclear weapon. And there are a lot of different ways to focus on this. One of course is to try and buy them all up overseas. That is an important job. We should do everything we can. It is next to an impossible job. It seems to me the better way to do this is to be at the choke point, that is, the place where a nuclear weapon would be smuggled into this country.

And I have been trying to push this Congress for years, and the administration now for 2 years, coming from the city from which I come, to do more on this. We had originally proposed—technologically it is feasible—to develop detectors that you could put on every crane that loaded a container bound for the United States, on every toll booth of a truck that entered our borders, and those are really the only two ways you can bring a nuclear weapon here into this country, that could detect an amount of radiation in a real bomb. I have been pushing to have money for this. We had proposed 150 million, which is what the scientists told us they needed the first year. We got 35 million through the Appropriations Committee, and even that, as best I can tell, has not been spent.

So here my question goes to all of the panelists, or particularly our two Commission members and Asa Hutchinson from Homeland Security. Should we not be doing more on this? Are we doing enough on this? Why, and to Asa in particular, why are we not spending at least the paltry $35 million that has been allocated to develop these devices? Is it good enough to inspect only 4 percent of the containers, for instance, that come through our ports, for nuclear devices?

Mr. HUTCHINSON. Thank you, Senator Schumer. First of all, we agree completely with the underlying point that we have to do all

we can to detect nuclear devices, weapons, material that might be coming into the United States. We have a goal of 100 percent radiological screening of cargo and conveyances coming into the country. We have deployed 151 imaging systems, detection systems. We have 10,000 personal radiation monitors that have been deployed, 284 radiation portable monitors. In reference to a dollar amount, the President's budget for 2005 asks for $50 million, which is an increase from what was previously designated.

And so we share the commitment, and we believe it is important, and we are working very hard to make sure that those items are procured and deployed.

Senator SCHUMER. Asa, I am glad it is 15 million more. Every expert will tell you that over a 3-year period—because I have talked to all of them, and none of them are terribly political, these are scientists. The idea is to develop something that moves from a Geiger counter to sort of a foolproof detection device that can detect things many more feet away. A Geiger counter works great at three feet. It does not work at 80 feet. And 50 million is not close to enough. We have faced so many dangers, and it is not an easy job. Look at the range of the questions, every one of them legitimate that has been asked here. But this is so serious in terms of its devastation, and it is hardly the most expensive even to implement and everything else. Why only 50 million? Why are we not doing more? And again, this is not just an al Qaeda problem. This is our problem for the next generation.

Mr. HUTCHINSON. That is correct. For example, whenever we looked at New York and concerns in that arena, we make sure that we have our assets flexible enough to deploy where they are needed to be.

Procurement is an issue whenever it is allocated. So the schedule of manufacturing and the procurement of that, but we are moving very quickly on that. And we are enhancing our capacity.

Senator SCHUMER. Why has the $35 million not been spent that was allocated not in this year's budget, but in last year's?

Mr. HUTCHINSON. I would have to get back with you on that. Customs and Border Protection is spending that money as quickly as they can in terms of procuring these assets. I mentioned the 151 that has been deployed, 284 radiation monitors. So there is a schedule that is being met day in and day out for the deployment of these radiation monitors.

Senator SCHUMER. But we still only do 4 percent of the containers and a certain percentage, I do not recall, of the toll booths. I have seen them work. I have seen the ones that are there. They are just not close to enough.

Chairman HATCH. Senator, your time is up.

Senator SCHUMER. Could I just ask our Commissioners to comment?

Mr. HAMILTON. Well, Senator Schumer, I want you to take a look at our proposal on the National Intelligence Centers. All of the attention has been on the National Counterterrorism Center, but we recommend, it is the other side of the chart here, all of the attention has been over here, but the other side of it is that the administration would identify the major threats to the national security of

the United States—counterterrorism would be a part of it—but also the weapons of mass destruction.

And you would put in one place then the authority to bring together all of the intelligence that we have from all of these various intelligence agencies, but more than intelligence, you would do operational planning there, and that follows the military example, where you pool J2 and J3 together. And so you would put in one place in Government the responsibility to plan operations to deal with weapons of mass destruction. You would have all of the intelligence the Government has. We support the expansion of the Proliferation Initiative of the President. We support more funding for the Cooperative Threat Reduction Program. This is the ultimate nightmare—

Senator SCHUMER. Right.

Mr. HAMILTON. —that the terrorists gets hands on a weapons of mass destruction. We know that they have tried for 2 years to do so, and it is a terribly important program. But take a look at the potential of the National Intelligence Centers as the way to deal with this problem.

Senator SCHUMER. Thank you, Mr. Chairman.

Chairman HATCH. I have a lot of questions that I will submit in writing, and I hope others will as well.

Senator Leahy would like to ask one or two more questions.

Senator LEAHY. Just because I thought that the line of questions that Senator DeWine was asking was a good one. I just want to make sure I fully understand this.

I will direct to you, Ms. Baginski. Am I pronouncing that right—"Baginski" or "Bajinski"?

Ms. BAGINSKI. Baginski is correct, sir. Thank you for asking.

Senator LEAHY. Hard "g." You said earlier the FBI can do multiple term searches in the Integrated Data Warehouse, the IDW. Now, I am not quite sure what databases are in there. Are case files included in that?

Ms. BAGINSKI. Yes, sir.

Senator LEAHY. So let us say you had a scenario like the well-known Phoenix memo, where the young FBI agent who blew the whistle on the potential hijackers taking flight lessons out in Phoenix, presented a memo that was basically shunted aside when it reached headquarters. If that was generated today by an agent in the field, would it be included in the IDW?

Ms. BAGINSKI. Yes, sir.

Senator LEAHY. Thank you.

Ms. BAGINSKI. I can give you a specific example from the demonstration they gave me on my first day here, which was to show this set of data that included a lot of different things, including case files, but not all case files, but terrorism information. And the activity was I could ask it a question. So I asked it give me information on how terrorists could do us harm. And with no fix in or anything else, the first thing that came up was the Phoenix memorandum.

Senator LEAHY. Maybe this fall Senator DeWine and I might have time to just go down and take a look at it.

Ms. BAGINSKI. We would love to have you come and look at what the power of putting data like that together is doing for our analysis.

Senator LEAHY. I know how shocked I was right after 9/11, when I went down to the Center. I have said this publicly and in fact I discussed it with President Bush at the time. He was equally shocked at the amount of paper, and rewriting, and rewriting—

Ms. BAGINSKI. Yes, sir. And we have more work to do, and just not to—

Senator LEAHY. I want to help. I mean, I am not here to criticize.

Ms. BAGINSKI. But I also want to tell you that I had the responsibility for information sharing. And through a policy board we are looking specifically at IDW and trying to add to the data sets that are in there. That is the point I want to make to you.

Senator LEAHY. Thank you. I will be down.

Ms. BAGINSKI. Great, sir. Thank you.

Senator LEAHY. Congressman Hamilton and Senator Gorton, you have recommended the National Intelligence Director, and you recommend that the NID be located in the Executive Office of the President. The question comes to my mind, would that give the NID sufficient independence?

And, secondly, also on the question of independence, do you want this NID—to serve at the pleasure of the President or have a set term similar to what we do with the FBI Director?

And, thirdly, you recommend giving the NID hiring and firing authority over the FBI's executive assistant director for intelligence, as well as budgetary control of the FBI's Intelligence Division. Does that assistant director then remain accountable to the FBI Director and the Attorney General or does she or whoever it might be became accountable to the NID?

These are sort of questions that, as I walked across the fields of my farm in Vermont, I was thinking about maybe because I was not wearing a tie.

[Laughter.]

Mr. HAMILTON. Well, they are very important questions, Senator. With regard to the location in the White House, the Executive Office, a little earlier I was talking about the necessity of integrating a lot of aspects of counterterrorism policy. Where do you do that? Well, I think it has to be done in or near the White House. It has to be done with the authority of the President.

Now, we do not want to get hung up on boxes here. Boxes are not the most important thing. Authorities are the most important thing. If you do not put it in the White House, where do you put it? I do not think it would be correct to put it in DOD or the CIA because those departments and agencies deal with very specific kinds of responsibilities, and what you need is a very cross-cutting responsibility here. You are going to be giving direction to the Secretary of State, and the Secretary of the Treasury, and a lot of other people.

So we recommend putting it in the White House. That is for you all to sort through, but if you do not put it there, where do you put it?

Senator SCHUMER. With a term or at the pleasure of the President?

Mr. HAMILTON. No, he serves at the pleasure of the President. This position is—he is the principal adviser to the President, and we think the importance of a good relationship between the President and the National Intelligence Director is crucial. So we say coterminous with the President.

Now, this question of independence is a genuine one. And we all know that politicalization of intelligence is a very, very difficult problem. Our analysis of that was that we had put into this system a very good means of competitive analysis, and we do not think that the locus or the geographical location of where the principal adviser to the President sits, whether it is in the Executive Office Building or somewhere else, maybe even in Vermont—is key.

Senator LEAHY. That is okay. We have got enough people.

[Laughter.]

Mr. HAMILTON. The danger of politicalization rises because of the functions and the relationships not the location of the person. And I do not see how anyone can look at the present system today—you just came out in the Senate here with this devastating report on "groupthink" in intelligence community. What that means is a lack of competitive analysis. So I do not think the status quo is encouraging with respect to competitive analysis.

What we do is we keep all of the independent analysis—State will have their analysis; Treasury will have their analysis; Energy will have theirs; Army, Navy, Marine Corps, they will all have theirs—there is no change there—they have their independent analysis. And then we emphasize the importance of open-source analysis as well, which we think adds to the competitive analysis. Everybody wants competitive analysis. Nobody wants politicalization of intelligence. All of us recognize how difficult it is to deal with both of these problems.

We believe, if you look at our system very carefully, the creation of the National Intelligence Director has a number of benefits which will strengthen competitive analysis and decrease the possibility of politicalization of intelligence. You cannot ever remove the prospect of politicalization of intelligence, but you can decrease it.

Senator LEAHY. You did not answer what happens with Ms. Baginski. Is she accountable to the FBI and the AG—

Mr. GORTON. Basically, she is going to be accountable—

Senator LEAHY. —or is she accountable to the NID?

Mr. GORTON. Basically, she is going to be accountable to both. As we said, we have affirmative, we have been very positive about this relationship in the FBI between intelligence and law enforcement and the fact that people who work in the FBI know something about both.

I think we ought to emphasize just one other thing, in addition to what Lee has said to you. We do not say that this National Intelligence Director should be a Cabinet officer because we do think intelligence, the collection and communication of intelligence and operational planning should be separated from policy. Cabinet members are policymakers.

Policies, with respect to what is done in the White House, should go through the National Security Council and should be those of the President. But, on the other hand, the President has got to trust this person who is the head of all intelligence, and that is the

reason we make those recommendations. But that person should not be a policy setter.

Chairman HATCH. Senator Schumer said he will take one minute, and then we are going to shut this down.

Senator SCHUMER. Mr. Chairman, I have a whole lot of questions.

Chairman HATCH. And you can submit them in writing.

Senator SCHUMER. I am mindful of people's schedules. I will do them in writing.

I am going to ask Mr. Hutchinson in writing, just from the Homeland Security, why this $35 million, paltry as it is, has not been spent yet or just to give me some details, in writing. He does not have to do it now.

My final question relates, it is to both the Commission and Ms. Baginski. I am still concerned about all of those Saudi flights that came about right after September 11th. Long before the Commission came out, I sat down with Dick Clark, you know, he gave me his little synopsis as to what happened. I know you talked to him. And this is one place, one of the very few places I am not sure I completely agree with the Commission's recommendations.

My question is this, not did every person who was on that flight get a check—they did. Somebody went and cleared them. I am not sure it was under the best of circumstances—I want to know who authorized the flight. How was it, especially when all planes were grounded, that this plane was able to take off, filled with Saudi nationals, including some people in the bin Laden family? It could not have been Dick Clark. I do not think he would have that authority. And so did you ask that question on the Commission? Did you get any answers? Is it not a relevant question to be answered?

And then Ms. Baginski, if she knows anything.

Mr. HAMILTON. Well, we looked into it as thoroughly as we could, Senator Schumer. And I suspect this is one of these questions that will be looked at a great deal more in the future. We found no evidence that any flight of Saudi nationals departed before national airspace was opened or reopened. We found no evidence of the involvement of U.S. officials at the political level in any decisionmaking on these flights.

What the testimony was, was that Dick Clark—this was a few days after—was just—

Senator SCHUMER. It was on the 13th.

Mr. HAMILTON. Yes.—just besieged with hundreds and hundreds of questions. And the FBI called up Dick Clark, and there had been a contact from the Saudi Embassy to the FBI. The FBI called up Dick Clark and said, "Is it okay to let these flights go out?"

And Dick Clark said, "Yes, if checks have been made" or whatever. In other words, it was not something that took a huge amount of his time.

And from what we know, we believe the FBI conducted a satisfactory screening of the Saudi nationals before their departure, including extensive interviews with regard to the bin Ladens, and there were a number of them. Now, our own independent check of the databases found no links between terrorism and the Saudis that departed. So that is where we came out on the investigation.

Mr. GORTON. And I emphasize that is after the fact.

Mr. HAMILTON. That is after the fact.

Mr. GORTON. That is what we did later during the course of our investigation.

Mr. HAMILTON. That is after the fact. That is where we are in the investigation.

Senator SCHUMER. But you do not know who authorized this, the early one, the 13th was one of the very first flights allowed. It was not that everybody was flying then again. You had to get specific authorization. And then there were others later. Like there was one the 19th, after everybody was flying again.

Mr. HAMILTON. Is that the one from Florida that came up you are talking about?

Senator SCHUMER. Yes.

Mr. GORTON. Even that early Tampa flight to Lexington was after the Tampa airport was opened to general aviation.

Senator SCHUMER. Did they not have to get approval? I thought, in those early days, there had to—in other words, all planes were flying then?

Mr. HAMILTON. The commercial airplanes, it took a little while longer than some of the general aviation to get cranked up to fly.

Senator SCHUMER. And any general aviation was allowed on the 13th?

Senator GORTON. They did not take off until the Tampa airport was opened.

Chairman HATCH. That has got to be it.

I want to thank each of you for being here. I thought this was one of the best hearings that I have observed in the Congress, and it is because of the four of you and those who back you up. I think you have been terrific. I think you have helped us to understand a lot of things we need to understand. We have only scratched the surface in some ways, so we will keep the record open for a week for written questions, and hopefully you can help us even further there, so that we can do our part of this and of course participate in all of the other parts of it as well, which this Committee does very well.

So we want to thank each one of you. I am sorry it has taken us so long, but it has been a very, very worthwhile hearing, and we are grateful to you.

With that, we will recess until further notice.

[Whereupon, the 12:18 p.m., the Committee was concluded.]

[Questions and answers and submissions for the record follow:]

QUESTIONS AND ANSWERS

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 1, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions posed to Ms. Maureen Baginski of the Federal Bureau of Investigation following Ms. Baginski's appearance before the Committee on August 19, 2004. The subject of the Committee's hearing was "The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security."

We hope that this information is helpful to you. If we may be of additional assistance in connection with this or any other matter, we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Responses of the Federal Bureau of Investigation Based Upon the August 19, 2004 Hearing Before the Senate Committee on the Judiciary Regarding "The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security"

Questions Posed by Senator Hatch

1. The 9/11 Commission has recommended that the position of deputy National Intelligence Director ("NID") for homeland intelligence be filled by either the FBI's executive assistant director for intelligence or the under secretary of homeland security for information analysis and homeland protection. Do you think this recommendation - by failing to specify precisely which official should hold the position - may create an unnecessary conflict between the FBI and the Department of Homeland Security ("DHS")? More generally, do you believe the FBI Office of Intelligence and the DHS Directorate for Information Analysis and Infrastructure perform similar functions, such that the heads of those entities would be interchangeable in the role of a deputy NID?

Response:

The FBI believes the Director of National Intelligence (DNI) should have one principal deputy. We believe the spirit of the 9/11 Commission recommendations can be better achieved through an intelligence coordinating council made up of NSC/HSC principals.

2. You have served in leadership positions within two different components of the Intelligence Community, the National Security Agency and the FBI. Moreover, you have had an opportunity to view the cooperation, or lack of cooperation, among intelligence agencies at the highest levels. If the 9/11 Commission's recommendations are adopted, you could end up serving as a deputy to the NID, as well as reporting to the FBI Director. Based on your experiences, do you think this type of "dual-hatting" can work? In your opinion, are there any conditions that might improve the likelihood of a successful merger of your potential NID and FBI roles?

Response:

We do not think a "dual-hatting" approach is the best answer. We are concerned about dual-hatting deputies who already have full time jobs, we may be replicating the situation underscored by the 9/11 Commission of intelligence community leaders having "too many jobs." In addition, maintaining the operational chain-of-command authority within the agencies that have the

fundamental intelligence and law enforcement authorities and missions is of critical importance.

3. In your testimony, you have said the FBI's core guiding principle is that intelligence and law enforcement operations must be integrated. The 9/11 Commission's Report also endorsed the importance of this integration.

a. While creating a separate career track for intelligence agents may foster much needed expertise, are you concerned that it may also engender divisions within the FBI workforce or recreate the "wall" between criminal and intelligence investigators?

Response:

We are creating an FBI Intelligence Service comprised of agents, analysts, linguists, and surveillance specialists. A change of this magnitude always carries risk and one of them, as you pointed out, is the unintentional rebuilding of walls. We have taken several steps to mitigate that risk: First, agents will always be agents. Second, we will require intelligence certification. In March, 2004, Director Mueller adopted a proposal to establish a career path in which new Special Agents are initially assigned to a small field office and exposed to a wide range of investigative experiences. This will allow them an opportunity to develop their investigative skills and expertise in several areas.

After approximately three years, agents will be transferred to a large field office where they will specialize in one of four program areas: Intelligence, Counterterrorism-Counterintelligence, Cyber, or Criminal. They will receive advanced training tailored to their area of specialization. Even though agents will be afforded the opportunity to specialize, they will also cross-train among the specialities. This flexibility and cross-training will greatly enhance the FBI's overall investigative capability while building an integrated, cohesive career intelligence service.

b. Aside from the multi-disciplinary training of new FBI agents and the intelligence certification of field office deputies, what additional steps, if any, is the FBI taking to ensure the continued integration of its criminal, intelligence and counterterrorism missions?

Response:

We are developing an intelligence certification program for several positions within the FBI, to include Special Agents, Intelligence Analysts, senior managers, and other intelligence personnel. Once established, this certification will be a pre-requisite for advancement to Section Chief or Assistant Special Agent in

Charge, thus ensuring that all FBI senior managers will be fully trained and experienced intelligence officers. We have also incorporated a specific core element for intelligence into the Special Agent and Supervisory Special Agent Performance Plans.

c. Do you have additional thoughts on how best to balance the development of a professional cadre of intelligence personnel at the FBI and the continued integration of the Bureau's criminal and intelligence missions?

Response:

A core guiding principle of the FBI is that intelligence is organic to our investigative mission. The development of an intelligence career service will strengthen the FBI's overall intelligence capability by providing a workforce - Agent, Intelligence Analyst, Language Specialists, and others - that is proficient in both the law enforcement and intelligence missions. In this way, our intelligence proficiency makes our investigations better.

d. If the FBI's Office of Intelligence is placed under the direction of the NID - as some have suggested - would this be an important step towards better coordination of the nation's intelligence program, or a step towards reestablishing the "wall" between intelligence and criminal investigators the USA PATRIOT Act has helped to remove?

Response:

As you are aware, the USA Patriot Act and the FISA enhancements have lowered the real and perceived walls between intelligence and investigations. This was a vital step in the strengthening of the nation's intelligence program and maximizing its benefit to law enforcement operations. As I discussed earlier, the FBI supported the creation of the DNI, which we believe will serve to more effectively coordinate and manage the activities of the intelligence community. As you know, the position of DNI was established by section 1011 of the "Intelligence Reform and Terrorist Prevention Act of 2004" (Pub. L. No. 108-458), and the President has nominated Ambassador Negroponte to that position. The DNI's authority will also help to avoid dual reporting, minimize confusion, and ensure accountability for each agency within the intelligence community. The DNI will also serve to centralize the management of intelligence requirements within the community. These functions will enable the FBI and other members of the Intelligence Community to execute their specific missions while operating in a coordinated, efficient manner.

Questions Posed by Senator Leahy

4. The FBI issued a press release on July 22 responding to the 9/11 Commission's recommendations related to the Bureau. Director Mueller praised most of the recommendations and outlined steps the Bureau is already taking to implement them. Are there any Commission recommendations that you do not agree with, and if so, why?

Response:

I am comfortable with the recommendations of the 9/11 Commission relative to the FBI's mission, role, and responsibility. We are gratified and encouraged that the Commission has embraced our vision for change and has recognized the progress that the men and women of the FBI have made to implement that vision. However, the FBI will need some latitude with respect to the recommendation to create a dedicated ASAC position for intelligence matters. In some cases, the size of the field office calls into question the need for such a position. We endorse the designation of a single senior authority for intelligence matters in the field, but prefer latitude concerning the level of that person.

5. When Director Mueller testified before this Committee on May 20 of this year, he told us that phase three of Trilogy, the so-called Virtual Case File System, would be completed by the end of this year. Just one month later, on June 25, the FBI announced that VCF would not be completed by the end of the year. Instead, the Bureau said it would take a more gradual approach to introducing VCF. The new plan is apparently to set up a sort of "VCF-lite" in a small number of sites – that is, a slimmed-down version of VCF, with a small set of its planned functions -- and then expand its capabilities and network from there.

a. What changed between May 20, when Director Mueller told us that VCF was on track to be completed by December, and June 25, when the FBI acknowledged that VCF would not be ready as promised?

Response:

At the time of Director Mueller's 5/20/04 testimony, the FBI was in the process of assessing the product being developed by the contractor. That assessment and the FBI's revised plan were completed by 06/25/04.

b. What is the current status of this project, and when will the entire system be in place?

Response:

Last June, after the FBI determined that the product delivered did not meet our needs, Director Mueller authorized a two-track plan to move us forward. Track One, also known as Initial Operating Capability (IOC), will test the Virtual Case File (VCF) prototype that has already been developed. Beginning in mid-January 2005 and through March, personnel in the New Orleans Field Office, the Baton Rouge Resident Agency, and the Criminal Investigative Division's Drug Unit at FBI Headquarters will use the prototype VCF as their document routing system. Employees will create electronic documents on standard FBI forms as they currently do but, instead of carrying paper copies to the supervisor's in-box and then to others for approval, employees will conduct this process electronically. The FBI plans to shut the prototype system down at the end of the test period.

The FBI hopes to accomplish several objectives with this test. First, we want to see how easy the graphic interface is to use and how the electronic workflow process works from a business perspective. Second, we want to see what impact the prototype system has on the performance of the new Trilogy network. Third, we want to see how training can be improved so that we can deliver the most helpful and user-friendly training possible Bureau-wide.

The FBI will additionally deploy and test an electronic interface with the current Automated Case Support (ACS) System that will allow personnel to access ACS data from the new, more user-friendly system. This interface will be a significant accomplishment that provides the foundation for a long-term solution.

Armed with these lessons and the new ACS interface, the FBI will move forward with Track Two - the development and delivery of a computer-based investigative case management system that will help the FBI meet its responsibilities to our country more efficiently. As part of the Track Two activities, the FBI has asked a new contractor to examine the latest version of the VCF as well as available off-the-shelf software applications and those designed for other agencies, to determine the best combination to meet the FBI's needs. In many ways, the pace of technological innovation has overtaken the original vision for VCF, and there are now existing products to suit the FBI's purposes that did not exist when Trilogy was initiated. The FBI has also asked a different contractor to review and verify users' requirements, because the mission of the FBI has evolved and there are new requirements for information and intelligence sharing.

The FBI is moving forward with a better understanding of its technical requirements and how to overcome technical challenges. We now have a strategic plan for IT, and we are building a strong Office of the Chief Information Officer

to improve oversight of IT projects, to strengthen oversight of IT contracts, and to ensure that IT investments fully support the FBI's current and future missions.

c. What is the current projection for the final, total cost of the project?

Response:

It is too early to estimate the total cost of the program.

6. John Brennan, the Director of TTIC, testified on August 23, 2004, about the need to build an integrated information technology architecture, accessible to all members of the intelligence community. Do you agree? How would VCF or the Integrated Data Warehouse fit into this new architecture?

Response:

We agree with the need to build a government-wide integrated information architecture as outlined in the President's Executive Order entitled Strengthening the Sharing of Terrorism Information to Protect Americans. In the FBI's work processes, VCF, or its successor software, will be ingest tools (like the Automated Case Support system is now) for the Investigative Data Warehouse (IDW). VCF or its equivalent will be the first point of ingest for investigative and intelligence information and for records collected by Agents and others. IDW then allows the data to be accessed, analyzed, and used in the production of intelligence. IDW minimizes the compartmentalization of intelligence and/or terrorism-related data developed by the FBI and would fit within this new architecture. It would also allow the interchange between agencies, with the proper security and access controls necessary to protect methods and sources.

7. I understand that, after many millions of dollars spent, FBI agents now have the capability of e-mailing each other over a secure network. But I also understand that many field agents are still unable to send secure e-mails to other federal government agencies, or to state and local law enforcement and other entities outside the FBI. Is that true? If so, why does the FBI lack this basic capability, and what if anything is being done about it?

Response:

The FBI is faced with a unique challenge every day. Unlike other law enforcement agencies, we are responsible for communicating with the IC, other federal agencies, and our state and local partners in regional jurisdictions as it relates to our intelligence, counterterrorism prevention and criminal investigative responsibilities. This levies an enormous challenge on our IT resources and staff

by having to provide communications access via three enclaves, or levels of correspondence.

As a result of the Trilogy infrastructure roll-out, the FBI fielded a secure network and modern workstations that permit secure SECRET level emails within the FBI using Microsoft Outlook. Trilogy also provided web access for MS Internet Explorer and FBI legacy applications access. This was a critical first step to modernizing the FBI infrastructure and enabling further information sharing.

Next, the FBI fielded the FBI Automated Messaging System (FAMS), which provides secure organizational messages across the Intelligence Community (IC) and Law Enforcement (LE) communities. The FBI is the first civilian agency to convert to the new Defense Messaging System (DMS), which will be the standard for future IC messaging and cables. FAMS and DMS will permit the FBI to send secure organizational traffic, including multimedia attachments, between any FBINET workstation and over 40,000 external organizations, around the world, in minutes rather than hours or days. This will replace the old teletype-based system that has been the foundation for organizational messaging since World War II. FAMS will replace our old paper-based system and will provide analysts and agents with near real-time messaging access at their desktops. The Secret-level FAMS began 24/7 operations on 12/15/04, currently has over 300 users, and will support all FBI users by the summer of 2005. The Top Secret/SCI version of FAMS is currently in testing and is scheduled to be available for general use by approximately that same time.

TS/SCI connectivity is being provided by FBI's new Sensitive Compartmented Intelligence Operational Network (SCION) which connects over 1,400 users at the FBI HQ to the IC via the Joint Worldwide Intelligence Communications System (JWICS). A pilot connectivity project was successfully completed to five field offices. SCION availability at the New York and Boston field offices was a vital element in the FBI's support of the Republican and Democratic National Conventions. SCION is a business tool used by both the FBI's Counterterrorism and Counterintelligence Divisions. It has enabled FBI personnel to perform their mission more efficiently and effectively. Some accomplishments include the FBI's contribution to the President's Terrorist Threat Briefing, TTIC On-Line, Situation Reports, Threat Matrix, TS FISA, and Intelligence Information Reports. SCION supports IC email and INTELINK-TS web access. Over 25 Gigabytes of information has been downloaded from FBI's SCION website. The FBI has received funding from Congress to begin and continue implementation of SCION in field offices.

The FBI has new Secret-level connectivity to the Intelligence and Homeland Security communities through the Department of Defense (DoD) Secret Internet Protocol Router Network (SIPRNET). At the beginning of 2004, the FBI had

SIPRNET presence with 50 stand-alone workstations and servers at 16 locations. In December 2004, the FBI worked with DoD to establish a direct connection between FBINET and SIPRNET through a secure, trusted gateway that provides SIPRNET-to-desktop capability at all workstations connected to FBINET. This is the first direct connection between FBINET and an external network in the Bureau's history. The number of authorized FBI users had expanded to 300 users as of January 2005.

State and local officials assigned to one of the 84 Joint Terrorism Task Forces (JTTFs) will have access to Secret email and web access to INTELINK-S through the FBI ICDM. Access to state and local officials in their home facilities will be accomplished through secure Sensitive But Unclassified (SBU) Networks such as Law Enforcement Online (LEO), the National Law Enforcement Telecommunications System (NLETS), the Justice Communications Network (JCON), the DOJ Regional Information Sharing System (RISS) Network, the Open Sources Information System (OSIS), and DoD's NIPRNET. FBI agent access to this set of interconnected networks will be accomplished through the FBI's SBU Network and LEO. The FBI continues to expand the FBI's SBU Network and LEO.

8. It has been nearly 3 years since Congress directed the Attorney General to prepare a comprehensive report on the FBI's translator program. It was included in the USA PATRIOT Act so that Congress could better assess the needs of the FBI for specific translation services, and make sure that those needs were met. While we have received some important data regarding the program, some fundamental questions have not been addressed. For example, what are the legal or practical impediments to using translators employed by other Federal, State, or local agencies, on a full, part-time, or shared basis? When can we expect the PATRIOT Act report to be issued?

Response:

The report required by section 205(c) of the USA PATRIOT Act was sent to the Committee on December 22, 2004.

The scarcity of qualified translators available to federal agencies, particularly among Middle Eastern and Asian languages, has been documented through several studies (these studies include the 1/31/02 GAO report referenced above and a 2001 report by the National Commission on Terrorism entitled, "Countering the Changing Threat of International Terrorism"). Since most agencies' demands for translator resources exceed the supply, the concept of sharing translators is not practical, because each agency's natural tendency is to preserve limited resources for its own use. Such sharing is further impeded by non-uniform proficiency testing and clearance requirements.

Intermediate and long-range benefits of pooling federal translator resources are possible, but only if each federal agency is equally committed to the aggressive recruitment of translators and/or to the internal development of translator resources through language training. Otherwise, scarcity issues will continue to pose barriers to translator sharing.

There would likely be immediate, though limited, benefits from the pooling of U.S. Intelligence Community (IC) and federal law enforcement translator resources in languages where demand is diminishing or shifting across agencies or where needs are sporadic. This is especially true when the lending agency has higher vetting and clearance standards than the receiving agency. For example, the FBI's current excess supply of Spanish contract linguist (CL) resources could be immediately absorbed by DEA, Immigration and Customs Enforcement, or ATF because of the rigorous vetting and clearance requirements of the FBI. However, it would often be difficult for the FBI to absorb the resources of those agencies because most DEA, Customs, and ATF translators are cleared only for access to law enforcement sensitive information and not to national security information.

At the state and local law enforcement level, translation services are typically provided by police officers whose language proficiencies are uncertified or by CLs. While the FBI reviews any opportunities for resource sharing carefully, in most cases the law enforcement officer or translator does not possess the requisite security clearance to provide services to the FBI. For example, when the FBI's Chief of Language Services recently met with the Deputy Commissioner of the New York Police Department (NYPD) regarding the feasibility of such resource sharing, the NYPD indicated that they did not want their officers to undergo polygraph examinations, thus precluding them from receiving Top Secret clearances.

9. What are the current needs of the FBI for specific translation services? Is the FBI translation program operating to your full satisfaction at this time?

Response:

Since the beginning of FY 2001, FBI audio and text translation requirements have increased by 51%. In several Middle Eastern languages, such as Arabic, collection has increased by more than 100%. Because of this increased demand, and despite an addition of several hundred translators during this period, unaddressed work remains in certain languages. Simply put, the growth in demand for FBI translation services has outpaced the increased translator supply.

The President's FY 2006 budget includes a $27 million enhancement to the FBI's language analysis program, supporting an additional 274 positions above the FY

2005 funded staffing level of 490 positions. This funding would greatly enhance the FBI's capacity to address intelligence collected in foreign languages in support of critical counterterrorism and counterintelligence investigations, provide the National Virtual Translation Center with a permanent staff of linguists, and fund an expected FY 2006 in the FBI's contract linguist program.

10. Earlier this year, Senator Grassley and I raised questions about the so-called "I-drive" -- a special computer drive where FBI agents save and store investigative documents and memoranda before they are reviewed and finalized by supervisors. In March, the FBI admitted that documents in the "I-drive" are not made part of the FBI's case files and are not routinely searched for materials that should be turned over to Congress or, when required by law, to defense attorneys.

a. Describe in detail what documents and other material are contained in the "I-drive."

Response:

Historically, many FBI field offices established their own naming conventions for the computer drives on which they maintained documents that had not been uploaded into FBI information systems. Standardization of information management included the recommendation that the "I" drive be used as the squad or unit directory and, because everyone on a squad or in a unit has access to this directory (including the Information Management Assistants (IMAs)), files to be shared within the squad or unit were to be stored on this drive. Primarily, the "I" drive is used as a temporary repository for documents awaiting uploading into the permanent electronic case file - not for official, finished documents subject to discovery. Official documents are saved to the "I" drive while undergoing final review before being made part of the permanent, and discoverable, case file. Once a supervisor approves the record copy (the paper version), it is provided to the IMA by putting it on the "I" drive; the IMA then retrieves this document from the "I" drive and uploads it into the Automated Case Support (ACS) system. This action deletes the document from the "I" drive. The official record of the FBI is still the paper document. Although the document in ACS can be used as a reference copy, the National Archives and Records Administration has not yet approved ACS as an official system of records.

b. What has been done to review the material contained in the "I-drive" both prior to and after February 2004, when the Associated Press wrote a piece highlighting the problem?

Response:

Media reports in the spring of 2004 indicated a possible connection between the Oklahoma City bombing (the FBI's investigation was called OKBOMB) and a series of Midwest bank robberies (this investigation was called BOMBROB), and reported that the FBI was looking at computer "I" drives for discovery documents that may have been overlooked. Although, in fact, the FBI was conducting an exhaustive investigation (including interviews of suspects and witnesses, forensic analysis, and time-line comparisons) to determine whether there might in fact be some connection between these cases, the FBI's Inspection Division was asked to conduct a special inquiry regarding the FBI's provision of documents to the OKBOMB defense team pursuant to the discovery process. This inquiry included review of allegations that documents stored on the FBI's "I" drive regarding BOMBROB would implicate that the BOMBROB subjects in the OKBOMB case as well.

The Inspection Division instructed all Divisions and Legal Attaché Offices to review their May 2001 certifications with respect to discovery in the OKBOMB case and determine if the "I" drives had been searched. Offices unable to reach this determination were directed to provide backup "I" drive tapes for the covered period (May 2001) to the Inspection Division for review. Twenty-five offices certified that the "I" drive had been searched pursuant to the May 2001 requirement; six offices advised that the "I" drive was not configured on their servers as of May 2001 or that the drive was not used. One office advised that it was confident that the "I" drive had been searched pursuant to the May 2001 requirement, but was unable to certify that and did not maintain a backup tape for that time period. Thirty field offices and two Legal Attaché Offices provided backup tapes of their servers.

The Inspection Division loaded the tapes to a dedicated server and searched the data using keywords associated with the OKBOMB and BOMBROB investigations, including the names of the subjects identified in both cases. This process, which took approximately one month, involved the electronic review of millions of documents, 15,200 of which contained one or more of the keywords. These 15,200 documents were burned onto a CD-ROM.

The Inspection Division then obtained a copy of the Zyindex database from the OKBOMB investigation, which contained 167,000 documents, and obtained a comparison of the 15,200 documents from the "I" drive tapes, the 167,000 OKBOMB documents, and the documents in the FBI's Automated Case Support system. This comparison identified 891 questionable documents.

A CD-ROM containing the 891 questionable documents was forwarded to the Oklahoma City Division. Based on their knowledge of the documentation

provided pursuant to the OKBOMB discovery process, the Oklahoma City Division was asked to determine whether any of these documents that should have been made available for discovery had, in fact, not been provided to the OKBOMB defense team.

The Oklahoma City Division advised that, of the 891 questionable documents, only four had not previously been reviewed by members of the OKBOMB Task Force. Two of the documents were first drafts of FD-302s that were later changed so they could be uploaded to the FBI's Automated Case Support system; one document was an FD-71 complaint form that mentioned OKBOMB and was generated by the Denver Division; and the fourth document was unidentifiable.

c. Were the existence and potential problems caused by the "I-drive" reviewed by the 9-11 Commission?

Response:

While the 9/11 Commission Report does not address the FBI's "I" drives, the 9/11 Commission did review the FBI's data automation and technology processes, finding its information systems "woefully inadequate" during this period (page 77 of the Commission's report).

d. Can analysts access data and documents on the "I-drive" through the Integrated Data Warehouse? If not, why not, and do you plan for this to change.

Response:

The purpose of the Integrated Data Warehouse (IDW) is to facilitate the analysis of data that has been collected and documented by FBI employees. While the IDW will utilize the FBI's network architecture to facilitate the analysis and sharing of data in FBI systems, it will not "see" or pull in data from the "I" drive. This is appropriate because the purpose of the "I" drive is to facilitate the mobility of the FBI's workforce by allowing employees to access their work-in-progress from any computer connected to the FBI network, and documents that have not been reviewed or approved by supervisors may contain inaccurate or incomplete information. If this information were made available to all analysts, they would risk the possibility of reaching incorrect conclusions based upon unverified data. Once a document is approved, it is uploaded into the FBI's Automated Case Support system, from which information is retrievable and searchable by all employees. Except as described in question 11c, below, these documents could then be accessed by analysts through the IDW.

e. Will the "I-drive" still exist once VCF is implemented? Please explain.

Response:

The "I" drive is a networked computer drive that allows computer users to retrieve items that they are working on from any computer connected to the network. This type of network architecture facilitates the mobile nature of the FBI's workforce, while providing the appropriate security for information and intelligence gathered by the FBI. These network drives are not designed as repositories of information; they are designed to facilitate work that is in progress.

Because VCF, or its successor software, will permit documents to be drafted, reviewed, verified, and approved by supervisors within the workflow process defined by that software, the current use of the "I" drive will no longer be required after that software is deployed. Even then, however, networked drives that allow FBI employees to access their work in progress from any networked computer will still be a necessary part of the FBI's Enterprise Architecture. Consequently, while these shared drives may be called "I" drives or may use some other naming convention, shared drives will continue to have utility in the FBI, though for different purposes than the "I" drive is currently used.

11. During your testimony, you said that "case files" were included in the Integrated Data Warehouse (IDW). It is my understanding that FBI case files include documents such as FD-302's (interview memoranda), electronic communications, documents obtained by the FBI in the course of an investigation (and filed in "1A" envelopes with the case file), transcripts of wiretap recordings, as well as other materials.

a. Please confirm that these items are included in a typical FBI "case file" and explain what, if any, other types of documents or materials are kept in a "case file."

Response:

The above listed items are kept in a case file. In addition to electronic communications (ECs), FD-302s (Form for information that may become testimony), and transcripts, other types of data stored in a case file include Facsimiles, FD-542s (Investigative Accomplishment Reports), Inserts, Teletypes, Letter Head Memorandums (LHM), Memorandums, and other miscellaneous documents.

b. Are all of these items accessible through the IDW?

Response:

Except for those items described below in item (c), all of these items are accessible through IDW.

c. What if any documents or materials kept or maintained in an FBI "case file" are *not* accessible in IDW, and why? Please be specific.

Response:

Most, but not all, electronic documents or materials kept in an FBI case file are accessible through IDW. A small number of case file documents that identify specific types of data too sensitive for all IDW users are not accessible through IDW. For example, information that reveals the identities of informants, information on public corruption investigations, and some administrative "case files" such as FBI employee disciplinary actions would not be accessible.

Prior to September 11, 2001, information in case files was primarily restricted to agents directly involved with the respective cases. Following September 11, 2001, Director Mueller established an "open data" policy, which permitted FBI analysts to access all data in FBI systems, with the exception of the most sensitive files identified by the EAD for Counterterrorism/Counterintelligence. This policy change allowed counterterrorism analysts to make more effective use of the FBI's collected data.

In accordance with the "open data" policy, the IDW system allows users to access all data in the system, although "need-to-know" principles still apply. The restrictions described above are intended to protect the FBI's most sensitive data from threats such as that posed by Robert Hanssen. To further protect against this type of threat, IDW audits all user activity.

As is further described in part (d) below, the FBI is aggressively developing a more advanced security system that would allow all documents to be included in the data warehouse, with strict protections applied to the most sensitive documents.

In order to ensure that FBI policies create the most effective counterterrorism environment possible, Director Mueller established an Information Systems Policy Board that is charged with reviewing existing policies, modifying policies when necessary, and establishing new policies as needed to respond to a changing environment.

d. For any documents or materials not accessible through IDW, please detail how the FBI currently searches for data in such documents or materials, and how or whether the search is conducted differently today than it was prior to September 11, 2001. For documents not currently accessible in IDW, when will the FBI will be able to access such materials electronically?

Response:

The documents not available through IDW are currently accessed through their original sources' systems, as they were prior to September 11, 2001. However, the access rules applied to these systems have changed in response to the events of September 11 to provide greater access and enhanced auditing features. This provides a greater ability to locate and disseminate data than the FBI had prior to September 11, 2001.

The FBI is actively working on a project based on the IDW system that will add a more robust security layer, which includes the detailed discretionary access controls required for the FBI's most sensitive files. The FBI anticipates completion of the testing and evaluation of the new technology in the summer of 2005. If additional funding is secured, the FBI will initiate the process of loading the excluded documents described in part (c) above into the system with appropriate protections. Access will then be expanded to the full user base of IDW.

e. Is it true that IDW access to materials in an FBI "case file" is limited to only that information that has been typed by an agent or support personnel into an FD-302 or other report?

Response:

This is not true. There is a great deal of information in IDW other than that which has been typed by an agent or support personnel into an FD-302 or other report. With only the exceptions described in part (c) above, users have access to all electronic data that is stored in ACS, as well as other paper records which have been automatically scanned and converted into computer text. These scanned documents include Bureau-generated documents related to terrorism, as well as other terrorism-related documents such as those seized in Afghanistan and Pakistan. Also large quantities of data from other agencies, including DIA, NSA, CIA, DOS, and FinCEN have been ingested into IDW.

f. Are all investigative materials obtained by the FBI by subpoena, by NSL or by other means always reviewed contemporaneously and summarized in report form, such that they are accessible through the IDW? If not, why not?

Response:

All investigative materials obtained by the FBI by subpoena, NSL, or by other means (such as that provided by 18 U.S.C. §2703) are reviewed contemporaneously. Not all investigative materials reviewed are deemed pertinent to a case. Those materials that are reviewed and deemed pertinent to a case are either summarized, in which the case summary is loaded into ACS, or the entire document is scanned, if necessary, and uploaded in its entirety into IntelPlus.

Many of the largest IntelPlus file rooms have been imported into IDW, so these documents would be accessible through the IDW in both text form and the original scanned images. Summaries loaded into ACS would be accessible through the IDW, except as noted in answer 11(c).

The only investigative materials that would not be available through the IDW are those that were not deemed pertinent to a case, those that were added to an IntelPlus file room that has not yet been incorporated into IDW, or those that are too sensitive to load into IDW, as described in answer 11(c).

g. What is the time frame for the dataset "case file" material that is currently accessible by IDW? In other words, are FD-302s that were written in 1995, 1990, or even prior to 1985 accessible?

Response:

The time frames for the datasets vary. Except as noted in part (c) above, all data stored in ACS, including FD-302s, are available in IDW. Since ACS was created in 1995, IDW contains ACS data from 1995 to present. IDW also contains millions of scanned paper documents, including those seized from suspected terrorists. Although the FBI knows the dates these documents were added into IDW, the date of origin of many of these documents is unknown.

As additional data sources continue to be added into IDW, most contain records dated prior to the date of ingest. All of this "day back" information will be included in IDW. The specific date ranges of the data will vary by source, and may include data prior to 1985. For example, IDW includes all CIA Intelligence Information Reports (IIR) at the Secret or lower classification levels issued from 1978 to present. Conversely, most data sources provide updates of new data created after the initial date of ingest. These "day forward" updates will continue to be added into IDW and appended to the appropriate data libraries.

h. You gave a "specific example" in order "to show this set of data that included a lot of different things, including case files, but not all case files, but terrorism information." Can you explain what you meant by this statement including the phrase "but not all case files, but terrorism information"?

Response:

The statement was intended to emphasize that the set of data includes terrorism information. The statement could be more clearly conveyed using two sentences: "The IDW included a lot of different types of data, including case files. IDW may not currently include all case file data (as discussed in question 11.c. above), but it does include terrorism information."

12. In early 2003, Director Mueller described the IDW as a future goal of the FBI that would encompass "31 different databases" and would be used to help the FBI conduct "data mining."

a. Please identify and provide a brief explanation of each database currently included in, or currently planned to be included in, the IDW. Approximately when was each database made accessible through IDW?

Response:

The following data sources are currently available through IDW. Other data sources that are planned to be added, pending approval by the Policy Board and the Office of General Counsel's (OGC) review of the Privacy Impact Assessment, are listed below in the response to (b).

Currently Included (Added Prior to January, 2004):

- Automated Case System (ACS), Electronic Case File (ECF)
- Secure Automated Messaging Network (SAMNet) – copies of all messaging traffic sent either from the FBI to other government agencies, or sent from other government agencies to the FBI through the Automated Digital Information Network (AutoDIN).
- Joint Intelligence Committee Inquiry (JICI) Documents – scanned copies of all FBI documents related to extremist Islamic terrorism between 1993 and 2002.
- Open Source News – various foreign news sources that have been translated into English, as well as a few large U.S. publications, such as the Washington Post.
- Violent Gang and Terrorist Organization File (VGTOF) – lists of individuals and organizations associated with violent gangs and terrorism, provided by the FBI National Crime Information Center (NCIC)

Currently Included (Added Between January 2004 and Present):

- 11 Financial Crimes Enforcement Network (FinCEN) Databases – data related to terrorist financing
- 2 Terrorist Financing Operations Section Databases - biographical and financial reports on terrorism-related individuals
- 11 Scanned document libraries – millions of scanned documents related to FBI's major terrorism-related cases
- CIA Intelligence Information Reports (IIR) and Technical Disseminations (TD) – copy of all IIRs and TDs at the SECRET security classification or below that were sent to the FBI from 1978 to present
- Foreign Financial List – copies of information concerning terrorism-related persons, addresses, and other biographical data submitted to U.S. financial institutions from foreign financial institutions
- Selectee List – copies of a Transportation Security Administration (TSA) list of individuals that warrant additional security attention prior to boarding a commercial airliner
- Terrorist Watch List (TWL) – the FBI Terrorist Watch and Warning Unit (TWWU) list of names, aliases, and biographical information regarding individuals submitted to the Terrorist Screening Center (TSC) for inclusion into VGTOF and TIPOFF watch lists
- No Fly List – copy of a TSA list of individuals barred from boarding a commercial airplane
- Universal Name Index (UNI) Mains – copy of index records for all main subjects on FBI investigations, except as mentioned in part (c) of question 11 above.
- Universal Name Index (UNI) Refs – copy of index records for all individuals referenced in FBI investigations, except as mentioned in part (c) of question 11 above.
- Department of State Lost and Stolen Passports - copy of records pertaining to lost and stolen passports
- Department of State Diplomatic Security Service – copy of past and current passport fraud investigations from the DOS DDS RAMS database

Planned Data Sources:

- (See part b below)

b. You stated in your testimony that the FBI "through a policy board" is looking specifically at IDW and trying to add to the data sets that are in there. How does the policy board operate and what other databases are being considered for inclusion in the IDW?

Response:

The Director created an Information Sharing Policy Group, co-chaired by the Executive Assistant Director - Intelligence and the Executive Assistant Director - Administration. This group reviews all requests for new data, as well as the dissemination controls imposed upon data sets. Before a data set can be approved by the policy board, or dissemination controls can be changed, the FBI's OGC must review and approve a Privacy Impact Assessment for the requested change.

Other primary data sources being considered include the FBI's Telephone Application, DHS data sources such as US-VISIT and SEVIS, Department of State data sources such as the Consular Consolidated Database (CCD), and Treasury Enforcement Communication System (TECS). Some of these sources will include very large amounts of data and funding has not yet been identified to complete their integration.

c. Does the FBI use IDW for "data mining?" If so, please describe the process, and indicate its effectiveness and reliability.

Response:

In its original statement, the FBI used the term "data mining" to be synonymous with "advanced analysis." The FBI does not conduct "data mining" in accordance with the GAO definition, which means mining through large volumes of data with the intention of automatically predicting future activities.

IDW allows for advanced analysis of large amounts of data, such as extracting all individuals from Suspicious Activity Reports and comparing the information against all individuals extracted from FBI terrorism investigations to look for overlap. All results are passed to FBI analysts for evaluation and further analysis. The FBI does not automatically generate predictions from IDW. Rather, it uses IDW to assist in identifying the most relevant elements of information that will allow trained analysts to make informed evaluations and predictions. This approach saves analysts valuable time in gathering information from various sources, and has proven highly reliable.

d. Can other government agencies (federal, state or local) access IDW and if so, how?

Response:

Other government agencies can access IDW through their representatives to FBI Joint Terrorism Task Force (JTTF) members. JTTF members, including many

federal, state, and local agencies, have been issued IDW accounts, and can access the system through any FBI computer connected to the FBI Intranet. These individuals must have completed background checks and been granted Top Secret clearances before they are granted access to FBI computers.

13. Do all FBI agents have access to the IDW on their desktops? If not, who has direct access to IDW? If agents do not have direct access, why not, and when can we expect them to have such access? Do you agree that it is important for the field agents to have access to all data at their fingertips in order to be able to react quickly in matters involving national security?

Response:

IDW is accessible from any FBI desktop; however, not all FBI agents have accounts. The Office of Intelligence Oversight Unit is responsible for evaluating user needs and prioritizing the creation of user accounts. Policy established by the Oversight Unit places priority on Field Intelligence Group members, and members of the Joint Terrorism Task Forces, in addition to the headquarters counterterrorism analysts that made up the initial user base. Since January 2004, IDW has issued more than 5,000 user accounts in accordance with the established policy.

The FBI agrees that it is important for field agents to have access to the data sets provided by IDW. The FBI intends to continue adding accounts and increasing the capability of the system accordingly; however, current funding does not support the provision of service to all FBI agents and analysts.

14. You also stated that the FBI can now do a "multi-word search" of data that is included in IDW. When was this capability made available through IDW? It is my understanding that these "multi-word searches" are still a long way from the type of multi-word searches that have become commonplace using the Internet or other search engines such as Lexis/Nexis or Westlaw. Thus, while the FBI can use multiple search terms like "flight school" and "lessons" to obtain some documents, it is my understanding that the FBI still cannot find words within a certain defined parameter of one another. There may also be significant limitations when variations of spelling are used. Please explain in detail the types of searches of IDW that are currently available to FBI agents and any types of searches that are not currently available that you plan to add. Please include a timeline for any currently planned improvements to the search capability of your computer technology.

Response:

IDW included multi-word search ability when it was activated January of 2004. It provides greater search capability than that available through the Internet. Users

can search for terms within a defined parameter of one another. For example, the search: 'flight school' NEAR/10 'lessons' would return all documents where the phrase "flight school" occurred within 10 words of the word "lessons." Users can also specify whether they want exact searches, or if they want the search tool to include other synonyms and spelling variants for words and names. Users can also combine all of these text search abilities with structured queries, such as limiting data by date ranges or FBI case classifications, within a single search.

IDW is also capable of extracting concepts such as names, phone numbers, and company names from unstructured text documents. This ability allows an IDW user the ability to perform concepts-related searches, rather than a list of documents. Users can then select concepts from the list, and browse through a series of related concepts that were extracted from the same document set. For example, a user could query information on a terrorist organization and retrieve a list of names extracted from documents about the terrorist organization. The user can then select a name from the list, and view a list of phone numbers extracted from the subset of documents that mention the selected name. At any point, the user can select a concept and view all related source documents for further analysis. This is a very powerful analytical method that is fundamentally different than standard search engines available through the Internet.

These capabilities are currently functional and available to all users. We are working on enhancing our ability to conduct multiple, large "batch queries." The example of advanced analysis provided in question 12(c), where the complete set of Suspicious Activity Reports is compared to the complete set of FBI terrorism files to identify individuals in common between them, is one type of "batch query."

15. The third phase of Trilogy - the Virtual Case File System, or VCF - was meant to replace the Automatic Case Support System (ACS). I took from your testimony that IDW is now adequately accessing ACS to ensure that all FBI information is capable of and is actually being mined for intelligence analysis and as an investigative tool. Many millions of dollars have been spent in preparing for VCF and millions more will be spent to see that it is implemented.

a. Why is VCF still necessary if IDW and ACS are doing the job?

Response:

IDW addresses a subset of FBI investigative data while VCF, or its successor software, will provide access to all data resident in ACS. VCF and its successor software will provide enhanced workflow and case management functionality

including the ability to search through various records, while that access is transparent to the user.

b. How (if at all) will VCF differ from IDW/ACS? In other words, will VCF be faster, easier, or more accessible to more agents and analysts? Will it have more sophisticated searching capabilities?

Response:

VCF, or its successor software, will far exceed the current ACS capabilities. It will essentially migrate the FBI from a "green screen" to a web interface, leaping several generations of technology. This capability will provide a faster and more user friendly interface for the agents and analysts. The greatly improved search capabilities will significantly improve their overall effectiveness and efficiency. VCF, or its successor software, also will contain a considerably larger repository of records than the IDW.

c. How is the continued delay of VCF's implementation adversely affecting the FBI's abilities?

Response:

The current paper-oriented workflow requires added time for data to be entered into the system of record, thereby delaying access to others. In addition, the lack of a search capability across records limits the FBI's ability to perform its intelligence and investigative functions. Despite the FBI's delay in implementing VCF, the FBI has achieved savings through the use of IDW.

d. The OIG noted in its September 2003 report that "unlike the currently used ACS system, agents will not be able to circumvent the use of the VCF." What do you understand that statement to mean and how does the ability of agents to circumvent ACS affect the IDW search engines?

Response:

Currently, the lack of controls with ACS prevents some users from submitting data in order to protect sources. VCF and its successor software will provide access controls that will require users to submit required data fields without later revealing critical source information to IDW users.

e. The same September 2003 OIG report stated that with the release of VCF, agents will be provided with "content management capability" to "help agents access information from the FBI's data warehouse, regardless of where in the system the

information was entered, [and] provide a single query for all of the FBI's systems that are connected to the Integrated Data Warehouse." Since VCF is still delayed, do the agents have this "content management capability" at this time and if not, when can we expect this capability to be in place?

Response:

Agents do not currently have content management capability.

16. The OIG once described VCF as a "web-based 'point and click' case management system" through which "agents are expected to have multi-media capability that will allow them to scan documents, photos, and other electronic media into the case file." Am I correct that the FBI does not have that ability at present and that, therefore, scanned documents, photos and other electronic media are not accessible through the IDW at this time?

Response:

The FBI currently has the ability to make scanned documents and other electronic media available through the IDW.

VCF, or its successor software, will simplify the process of scanning documents and photos, and adding other electronic media into the case files, but it is still possible with current systems. Agents can use scanners provided by Trilogy, as well as the more robust services provided by the Document Conversion Laboratory (DOCLab) and Document Exploitation group (DocEx) to convert data into electronic form. Millions of these scanned documents have already been loaded into IDW and are available to users. In addition to scanned document libraries, the Violent Gang and Terrorist Organization File (VGTOF) library already has photographs imbedded with the electronic records and are accessible through IDW.

17. Earlier this year, with Senators Hatch, Grassley and Durbin, I asked the Government Accountability Office (GAO) to review the approximately $600 million in costs attributed to the Trilogy system, which is still not in place. Can you assure me the FBI is fully cooperating with the GAO's audit, and doing so on a timely basis? Please explain what you are doing internally to ensure that the GAO is getting the materials it needs.

Response:

The FBI has and will continue to cooperate fully with the GAO auditors by providing timely, accurate, and complete information. Materials and information in response to GAO's requests have been provided. As an interim step to ensure

the GAO is receiving the requested material in a timely fashion, in lieu of waiting until all material in response to a single request is available, the FBI will provide the information incrementally.

18. The September 2003 OIG report on Trilogy also commented upon the problems at the FBI regarding entry of foreign names into the FBI's existing databases (ACS) and explained that VCF would facilitate indexing on various web-based documents by providing data fields in searchable databases.

a. Does this mean, for example, that a VCF search of materials about Moammar "Gadhafi" will yield reports that spell the Libyan leader's name as Qaddafi, Qatafi, Quahthafi, Ghadafi, Kadafi or Kaddafi?

Response:

The VCF design included a wildcard search ability, but in its initial release would not have searched across name variants. In later releases, VCF was planning to incorporate Language Analysis Services (LAS), which has a robust name expansion utility to provide this service.

IDW has partially integrated LAS, and has already used it to support critical investigations, such as the 2003 holiday threat. This allowed IDW to expand a name into alternate spelling variants for comprehensive searching and analysis. This capability continues to be available to support special cases, and IDW plans to complete the integration and expose the name expansion capability to end users in a future release. Current funding, however, does not include this integration. At present, IDW allows users to manually create name expansion lists that would allow IDW to search across all identified variants. If LAS were fully integrated, users would have the option of manually creating a list, or using the automatic expansion provided by LAS.

b. Regarding IDW's capabilities as you described them in your testimony, are fundamental spelling issues still causing problems in search engines? Please explain how, if at all, VCF will rectify this situation.

Response:

IDW includes the ability to search across spelling variants for common words, synonyms and meaning variants for words, as well as common misspellings of words. If a user misspells a common word, IDW will run the search as specified, but will prompt the user to ask if they intended to run the search with the correct spelling. In addition, users can create a list of name variants they wish to use and IDW will search across all identified name variants. As mentioned in the question

18(a), it is anticipated that VCF (or its successor software) and IDW will incorporate the capabilities provided by LAS that would provide automatic expansion of name variants.

19. On April 8, 2004, the Subcommittee on Terrorism, Technology and Homeland Security of the Senate Judiciary Committee held a hearing on "Keeping America's Mass Transportation System Safe: Are the Laws Adequate?" At that time, I posed a written question to the Amtrak representatives about whether or not rail police have direct access to law enforcement records systems while performing pedestrian and vehicle investigations. A copy of Amtrak's response is attached as Exhibit A to these Written Questions. Please provide your position on the legislative proposal suggested by Amtrak in which rail police that are certified and commissioned law enforcement officers would be provided equal footing with state and local law enforcement for purposes of access to criminal history data.

Response:

28 U.S.C. § 534(4)(d)(1) authorizes the Attorney General to exchange records and information with railroad police departments which perform the administration of criminal justice, have arrest powers pursuant to a state statute, allocate a substantial part of their budget to the administration of criminal justice (defined in 28 C.F.R. Part 20, Subpart A), and meet the training requirements established by law or ordinance for law enforcement officers.

Under this authority, upon request, the FBI assigns Originating Agency Identifiers (ORIs) to railroad police departments meeting the criteria of 28 CFR Part 20. A National Crime Information Center (NCIC) ORI is a nine-character alpha-numeric identifier assigned to authorized agencies, permitting access to the NCIC Interstate Identification Index (III). Amtrak has been assigned eight ORIs that permit access to NCIC/III for criminal justice purposes.

While railroad police are authorized to access the NCIC/III, each state determines whether to grant railroad police direct access to the NCIC/III through that state's system.

The FBI has no comment on the proposed legislation, which concerns access to state criminal history databases.

Questions Posed by Senator Feingold

20. The Commission report has focused on the need to improve sharing information within the federal government. But I am also concerned about how risk and intelligence

information is communicated between federal and local authorities. The federal government appears to be making some progress in getting information down to the local level. But some local officials have told me that they have no good way of getting information up to the federal level in an efficient and meaningful way. Local police are a potentially vast resource of information if we can figure out a way to effectively synthesize and use that information. The Joint Terrorism Task Forces (JTTFs) are one link between federal and local law enforcement. Beyond JTTFs, are there plans to tap into this resource or plans to expand the JTTF capacity to deal with the vast amount of useful information obtained by local law enforcement?

Response:

Yes, the FBI has worked hard to enhance its ability to be a strong node on the information network of the 800,000 strong state, local, and tribal law enforcement community, who are the first to encounter and defend against the threats that face the nation. The FBI has established Field Intelligence Groups (FIGs) in each of our 56 field offices to provide the bridge to and from our state, local, and tribal partners. The FIGs integrate analysts, agents, linguists, and surveillance personnel in the field to bring a dedicated team focus to intelligence operations and to serve as a conduit of information with our state, local and tribal partners. FIGs established partnerships with their state, local and tribal partners to assist them in developing their intelligence requirements. We placed an intelligence reporting capability in our Joint Terrorism Task Forces (JTTFs) to ensure vital information is flowing to and from those who need it. The FIGs also participate in Regional Intelligence Centers and other multi-agency intelligence initiatives to facilitate the information sharing process on a regional and local basis. We have more work to do to achieve the two-way flow of information we require to safeguard the nation, but our FIGS are designed to ensure that flow.

21. As you know, Director Mueller has stated that the FBI needs to recruit individuals who bring specialized skills, including cultural and language skills. The 9/11 Commission has also called on the FBI to implement a program to recruit, hire, and retain agents and analysts with backgrounds in intelligence, international relations, language, technology, and other relevant skills. The Commission found that one reason the FBI strategic analysis faltered was the FBI's tradition of hiring analysts from within, rather than recruiting individuals with the relevant, specialized educational background and experience.

a. What steps will the FBI take to implement this part of the Commission's recommendation to ensure that individuals with the best, most relevant skills are recruited for analytical and agent positions?

Response:

The FBI has taken several steps related to the Commission's recommendation to implement a recruiting, hiring, and selection process that enhances its ability to target and attract individuals with educational and professional backgrounds in intelligence, international relations, language, technology, and other relevant skills. The FBI has established recruiting bonuses and relocation reimbursement benefits to prospective Intelligence Analysts who have the critical skills we need. We have changed the list of "critical skills" for special agent recruits to include intelligence experience and expertise, foreign languages, and technology. We are also developing a National Recruitment Strategy to target and attract special agent and analyst candidates with professional intelligence backgrounds.

Once we attract and hire these candidates, we must train them, mentor them, and provide opportunities for career growth. We have taken a number of steps in that regard as well. We have adopted seven core learning objectives for the intelligence discipline relevant to both new agents and new analysts.

The Basic Intelligence Analysts training course was revised and updated to incorporate key knowledge elements of our intelligence program. This new course, ACES I, began on September 13, 2004. Additionally ACES I will focus on assimilation, analytic trade craft and practice, thinking and writing skills, resources, and field skills. An advanced analysis training course entitled ACES II is planned for the near future. This course will target more experienced analysts and will provide training for more complex analytic issues. Practical exercises and advanced writing skills will be emphasized, as well as advanced analytic techniques.

The New Agents training curriculum is being modified to incorporate the core intelligence learning objectives, supported by joint practical exercises with Intelligence Analyst trainees.

The FBI Training and Development Division is now identifying and engaging in intelligence training partnerships with other government agencies, academia, and the private sector to support its contributions to our intelligence career service.

Your question is aimed at the most critical issue in the development of the FBI's intelligence capability - its people. I focus on this issue daily, for without the human talent for intelligence production, business processes, policies, and technology enablers are dramatically reduced in their effectiveness.

b. How can Congress be helpful in the FBI's efforts to recruit the best and brightest at all levels of the agency?

Response:

The recently passed Federal Workforce Flexibility Act, Intelligence Reform and Terrorism Prevention Act of 2004, and Consolidated Appropriations Act for FY 2005 provide significant personnel flexibilities and will greatly assist the FBI in its recruitment and retention efforts. In addition, existing grant programs, such as the Senator Pat Roberts Grant Program for students in critical intelligence related fields, are invaluable to the FBI's efforts to recruit the best and the brightest at all levels. The FBI currently has six students who have been selected for the initial pilot program. The FBI looks forward to continuing its work with DOJ and the Congress to ensure that no unnecessary roadblocks exist in our ability to recruit, train, develop, and retain FBI employees who support our intelligence and other critical responsibilities.

22. Richard Clarke, the Administration's former top Counterterrorism official, has complained that the FBI has a tradition of mid- and senior-level managers who joined the FBI at a young age and have worked their way up, which, he believes, has created uniformity, insularity, risk-aversion, and an inability to think creatively "outside the box." What steps will the FBI take to ensure that the best qualified individuals, whether from inside or outside the agency, are hired for these very important positions?

Response:

Subsequent to the events of 9/11/01, the FBI has undertaken an aggressive approach to ensure that creative, innovative thinking is consistently fostered and comprehensively embraced at all leadership levels. First, an entirely new Special Agent Mid-Management Selection System was developed and implemented in June 2004, which requires mid-management candidates to provide specific, verifiable examples of their achievements based upon experiences both within and outside of the FBI, when applicable. The relative value of these accomplishments is assessed through the application of standardized rating criteria which accord the highest, most competitive rating of "Exemplary" to candidates whose accomplishments in top priority program areas such as Counterterrorism, Intelligence, and Counterintelligence clearly indicate that they have initiated innovative investigative or managerial approaches to address a variety of challenging problems. The new selection system characterizes innovative approaches as being identifiably different from those generally or previously utilized, representing a departure from more conventional or previously established approaches and exemplifying the application of creative thinking within the framework of Federal law. The competitive advantage provided by the exemplary rating represents a powerful incentive toward the development of innovative thinking and fosters an environment in which even the most experienced employees are encouraged to exercise their own creativity and fully

embrace the implementation of new ideas and methodologies. This emphasis on innovative action ensures the expansion of a management candidate pool characterized by a willingness and ability to think "outside the box." In addition to this, to date, over 250 FBI executives and senior managers have attended the highly prestigious Kellogg School of Management. This program has included such topics as Organizational Change, Effective Interagency Coordination, Strategic Thinking: Anticipation and Managing Public Perception, and Leading Individuals and Teams: Effective Decision-Making and Communications.

The other integral component of the FBI's approach demands that executive management positions be consistently filled with exceptionally well-qualified individuals possessing proven track records of creative, goal-oriented, and successful leadership. This initiative has required the FBI to clearly identify and enumerate the most vital competencies required for effective performance in its most demanding executive management positions, and then match these requirements to the unique qualifications of exceptional individuals sought from a variety of fields and industries. The FBI's current Senior Executive Service ranks comprise numerous executives drawn from a variety of other government agencies and major corporations, including the Executive Assistant Director for Intelligence, the Chief Information Officer, the Information Technology Operations Chief, and Assistant Directors for Investigative Technology, Security, and Training and Development. Succession planning efforts have additionally made substantial progress in further developing uniform competency requirements and addressing challenges inherent in the establishment of specific career tracks and the retention of the Bureau's most effective executive managers.

QUESTIONS FROM CHAIRMAN HATCH
SENATE JUDICIARY COMMITTEE
"THE 9/11 COMMISSION AND RECOMMENDATIONS FOR THE FUTURE OF FEDERAL LAW ENFORCEMENT AND BORDER SECURITY"
AUGUST 19, 2004

Questions for Under Secretary Hutchinson

1. It appears that one of the major weaknesses in our security system involves the interoperability of communications and coordination between various agencies in the federal government and those at the state and local level. For example, at the World Trade Center and Pentagon sites there were numerous law enforcement and emergency rescue personnel who quickly and heroically responded to the scenes. Nevertheless, the Commission Report highlights the lack of communication and coordination among these responders as a significant problem. What steps has the Department taken to coordinate the communication systems used by state and local first responders and federal agencies?

   Answer: The tragic events of 9/11 clarified the critical importance of effective first responder communication systems. Two major interoperability initiatives within the Directorate of Science and Technology of the Department of Homeland Security (DHS) have been established to address the interoperability problem: SAFECOM was established two years ago as a Presidential E-Gov Management Initiative (and a DHS responsibility since the summer of 2003); the Office of Interoperability and Compatibility (OIC) was established officially on October 1, 2004. The Department of Homeland Security is working aggressively to improve communications interoperability in both the near and long-term for public safety first responders through the SAFECOM Program.

   Communications interoperability refers to the ability of emergency response agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, as authorized. Unfortunately, the nation is heavily invested in an existing infrastructure that is largely incompatible. Currently, efforts within the Federal Government to address the interoperability problem are being coordinated by SAFECOM to incorporate the needs of local, state, and federal practitioners.

   SAFECOM's mission is to serve as the umbrella program within the Federal Government to help local, tribal, state, and federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications. By coordinating and building upon the vast range of interoperability programs and related efforts spread across the Federal Government, SAFECOM is reducing unnecessary duplication of programs and spending and ensuring consistency across federal activities related to research, development, testing and evaluation (RDT&E), standards, technical assistance, training, and grant funding related to interoperability.

   The SAFECOM Program is focusing on three key areas to build the foundation for a longer term, comprehensive interoperability program: the creation of an Architectural Framework, the development of standards, and the coordination of federal activities.

SAFECOM's architectural framework, the first version of which is expected to be published in the third quarter of FY 2005, will determine priorities for the development of standards. It is driven by the SAFECOM Statement of Requirements (SoR) version 1.0, which was released in March 2004, and will encompass successful techniques used by local, state, regional, or federal integration networks. This framework will reflect a system-of-systems approach to develop interface standards to help improve the problem of communications interoperability.

As part of the long-term strategy for improving communications interoperability, SAFECOM is closely coordinating the development of interoperability standards in partnership with local, state, and federal emergency response organizations to define the requirements for first responder interoperability at all levels. SAFECOM, building upon the SoR developed and published earlier this year and the Architectural Framework, is supporting ongoing efforts or, when necessary, initiating the creation of standards to address gaps where identified.

With input from the emergency response community, SAFECOM has created coordinated grant guidance that outlines eligibility for grants, the purposes for which grants may be used in support of interoperability, and guidelines for implementing a wireless communication system. This guidance was included as part of the COPS and FEMA grants in FY 2003 and was incorporated into the COPS Interoperability grants and Office for State and Local Government Coordination and Preparedness (OSLGCP) state grants in FY 2004. Interoperable communications investments have been the top priority for many DHS grant recipients, with over $800 million in DHS grant funding allocated for such efforts in FY04 alone.

DHS recognizes that communications interoperability is a long-term problem with no one-size-fits-all solution. For this reason, the SAFECOM Program has partnered with state and local practitioners to develop short term initiatives that will address communications interoperability.

Begun by Secretary Ridge in early 2004, the RapidCom Initiative has provided assistance to ten key urban areas to strengthen their ability to respond to immediate emergencies. This effort has also served as the catalyst for these areas to begin to institutionalize routine training and exercises, governance meetings, standard operating procedures, and more frequent use of interoperable communications in non-emergency situations to better prepare themselves for emergencies.

Another DHS near-term effort involves SAFECOM's work with the Commonwealth of Virginia to develop a strategic plan for statewide communications interoperability. The Statewide Communication Interoperability Planning (SCIP) Methodology developed out of the Virginia strategic plan and serves as a model for any state or region interested in developing a successful strategic plan for interoperability. The SCIP Methodology details key phases and steps in the process toward developing a statewide interoperability plan and has been made available to the emergency response community.

2. This summer, a group of Syrian "Musicians" flying from Detroit to Los Angeles raised concerns among some on their flight after exhibiting suspicious behavior. Upon arrival in Los Angeles, the musicians were greeted by the Federal Bureau of Investigation ("FBI") and Federal Air Marshals, but apparently officials from U.S. Immigration and Customs Enforcement ("ICE") were not among the first at the scene. The immediate response of ICE agents would likely have helped to resolve some of the travel document and immigration status issues involving these passengers, which have been reported in the press.

    a. How are we managing the coordination of agencies, communication, and information when a security incident occurs? Does the Department have policies and procedures in place, or agreements with other Departments such as the Department of Justice, in order to get the right people and the correct information to the scene as quickly as possible?

    Answer: The National Response Plan (NRP) is the overarching document for management of incidents of national significance and related incidents used by the Federal Government pursuant to Homeland Security Presidential Directive 5. Pursuant to the NRP, the Homeland Security Operations Center (HSOC) is currently developing communication and coordination Standard Operating Procedures which will be disseminated for coordination throughout the Federal Government.

    The HSOC is the primary national-level hub for domestic situational awareness, common operational picture, information fusion, information sharing, communications, and coordination pertaining to the prevention of terrorist attacks and domestic incident management. The HSOC collects and fuses information from a variety of sources everyday to help deter, detect, and prevent terrorist acts. Operating 24 hours a day, 7 days a week, 365 days a year, the HSOC provides real-time domestic situational awareness and monitoring of the homeland as well as coordination of incidents and response activities.

    The HSOC represents over 35 agencies ranging from state and local law enforcement to federal intelligence agencies. Information is shared and fused on a daily basis by Intelligence agencies and federal, state, local, and tribal law enforcement agencies. The Intelligence agencies focus on pieces of highly classified intelligence and how the information contributes to the current threat picture for any given area. The Law Enforcement agencies track enforcement activities across the country that may have a terrorist nexus. These two pieces fused together create a real-time snap shot of the nation's threat environment at any moment.

    In addition, the HSOC supports incident communications and coordination through a combination of: (1) the Senior Watch Officer immediately interacting with appropriate agencies; (2) desk officers from the interagency community assigned to HSOC exchanging information between their home agency's operations center and HSOC; (3) use of the Homeland Security Information Network (a sensitive but unclassified data network for exchanging incident, threat

and suspicious activity information between agencies engaging in Homeland Security missions); and (4) an established network of points of contact within various federal, state, county, local and tribal agencies with homeland security missions. HSOC facilitates such coordination and communication. HSOC does not obligate resources or unilaterally direct the commitment of other agency resources.

Major incidents requiring large-scale interagency coordination are usually handled by the DHS Integration Staff (I-Staff) in coordination with the HSOC and the Interagency Incident Management Group (IIMG). DHS has developed policies and procedures addressing the roles and responsibilities of the IIMG. When the IIMG is activated, the HSOC supports the IIMG by providing IIMG members with responses to their requests for information.

Additionally, Area Maritime Security Committees and Area Maritime Security Plans have been established in the port areas throughout the country. These Committees provide a framework to communicate threats, identify risks, and coordinate resources to mitigate vulnerabilities and threats among appropriate federal, state, and local agencies as well as port stakeholders at the local level. The Area Maritime Security Plans contain specific sections for communicating threat information, prevention of incidents through implementation of protective measures at varying threat levels, and organizing appropriate entities for response to security incidents. The Plans further define relationships, authorities, coordinating procedures, and resources available for response to security incidents.

b. What was the immigration status of the Syrian "Musicians" at the time of their flight?

Answer: At the time of the June 29, 2004 incident, the petition for extension was pending adjudication. The request for an extension to their visas was approved July 6, 2004, and because the extension was accepted as timely filed, it covered the period from when their visas expired, June 11, 2004 to July 15, 2004. All 13 musicians had hits due to NSEERS registration, but all security checks were done and resolved.

3. The 9/11 Commission Report describes the mobility of the 9/11 terrorists, and notes that "travel documents are as important as weapons" to terrorists. As the Commission points out, the 9/11 terrorists traveled to countries throughout the world to attend terrorist training camps and clandestine meetings. Often, however, they would return to their native countries and apply for entirely new passports, so the multiple "entry-and-exit" stamps from suspect countries would not be revealed to future border inspectors. This represents a multi-faceted problem that involves the travel document issuance and screening procedures of countries throughout the world. Biometric initiatives may eliminate certain aspects of the problem, but only if they are widely adopted and strictly enforced.

a. What is being done with the international community as a whole to ensure that travel histories are accurately recorded in passport documentation?

Answer: Having an accurate travel history available reflecting the movement of specific travelers is an important component of the risk assessment process. DHS has taken steps to ensure that such travel histories are available as we seek access to Passenger Name Records (PNR) from airlines worldwide. We have been successful in this endeavor, signing a groundbreaking agreement with the European Union which allows such access while addressing privacy concerns. This PNR information, which can include specific data relating to passports, is then used by DHS, most particularly CBP's National Targeting Center (NTC), as part of an overall regime of risk assessment and management to ensure our borders remain safe and secure. In addition, CBP Officers review travel indicated by cachets (entry or exit stamps) in passports and question travelers about prior travel, be it to the United States or elsewhere. CBP has access to an extensive library of altered and counterfeit cachets which are detailed for officers by U.S. Immigration and Customs Enforcement's Forensic Document Lab.

b. What safeguards, if any, exist to ensure that someone who applies for a visa to visit the United States has not exploited loopholes in his or her own country's passport process?

Answer: All applicants for a visa to enter the United States are interviewed by consular officers from the Department of State, who also check the applicant against various lookout databases to ensure there is no adverse information including information that would indicate a lost or stolen passport. In the course of this interview, the passport presented by the applicant is also examined, and the consular officer may ask detailed questions regarding how and when the passport was obtained. Fingerprint checks as part of the visa application prevent any previous visa applicant from obtaining a visa using a passport issued in a different identity. The addition of facial recognition technology to the visa process will provide a further safeguard against abuses of the passport systems of other countries. Additionally, many foreign governments provide information on lost and stolen passports to the Department of State. The Secretary of State, in coordination with Secretary Ridge, created an interoperable electronic system that allows for access of lost and stolen passport data (both U.S. and foreign) by consular, law enforcement and intelligence entities.[1] Further, in June 2004, the Department of State initiated a program, in coordination with DHS, to improve our ability to share lost and stolen passport data with foreign governments.[2]

An additional layer of screening is provided in certain countries (e.g., Saudi Arabia) by DHS staff stationed in those countries to conduct additional security

---

[1] Implementation of The Enhanced Border Security and Visa Entry Reform Act of 2002, section 308 of P.L. 107-173.

[2] Frank E. Moss, Deputy Assistant Secretary for Passport Services Bureau of Consular Affairs, Address to the International Relations Committee, U.S. House of Representatives (June 23, 2004).

screening. Finally, each CBP inspecting officer at our ports of entry conducts a de novo examination of the applicant for admission, including a review of the documents presented and, if necessary, questioning regarding how the document was obtained.

The United States drafted a document titled "Minimum Security Standards For The Handling and Issuance Of Machine Readable (and other) Passports (Recommended Standard Practices For the World's Governments)" that sets out in detail the ways in which governments can and should protect their passport issuance process. The document has been adopted by the International Civil Aviation Organization, the Organization for Security and Cooperation in Europe, and by the economies of the Asian Pacific Economic Council. As governments meet these minimum standards, loopholes in their passport process will be closed.

4. On August 17, 2004, *The Washington Times* published an article concerning the arrest of illegal aliens in Southern California, According to the article, intelligence from local police officers and residents led a U.S. Customs and Border Protection ("CBP") Mobile Patrol Group to arrest 450 illegal aliens at public places within California, The article suggests that you later "criticized the arrests, saying they had not been approved by officials in Washington and violated, . . [CBP] policy." CBP Commissioner Robert Bonner, however, reportedly said the arrests were within the Border Patrol's jurisdiction.

   a. Did you criticize the Mobile Patrol Group's arrests of these aliens who had successfully entered our country illegally? If you did, why would you criticize an effort that appears to have been successful?

      Answer: The Border Patrol is legally authorized by the Immigration and Nationality Act to interdict and apprehend individuals illegally in the United States. Although faced with an enormous challenge, through a unified presence, focus and determination, the Border Patrol is deploying a comprehensive national strategy on border enforcement.

      The U.S. Immigration and Customs Enforcement (ICE) has lead responsibility for interior enforcement operations "outside the proximity of the border." Border Patrol operations "outside the proximity of the border" that target aliens considered "domiciled" are not necessarily prohibited but will be appropriately coordinated with ICE and approved at the Headquarters level before commencement. My statement on the work of the Mobile Patrol Unit was based upon the policy guidelines issued by Commissioner Bonner.

   b. Given the 9/11 Commission's observations concerning our porous borders and lack of border security, and the apparent acknowledgement by ICE officials that they lack sufficient personnel or resources to carry out extensive interior enforcement programs, doesn't it make sense to use innovative programs, such as the Mobil Patrol Group, to enforce our nation's immigration laws?

      Answer: The Border Patrol has primary responsibility specifically for monitoring and responding to illicit border intrusions across approximately 8,000 miles of

border between U.S. Ports of Entry. Border Patrol operations focus primarily on routes of travel; egress; and transportation hubs (airports, bus stations, etc.) where there is a clear nexus to "border control." CBP will continue to work closely with ICE in a coordinated effort in securing our homeland.

5. You will recall that, at the hearing, Senator Kennedy discussed problems with getting off of the so called "no-fly" list. I have a constituent, named David Nelson, who flies once a week from Utah and is apparently also on a "no-fly" list. What procedures are in place to remove from "no-fly" lists the names of those individuals who can clearly and unequivocally show, like Mr. Nelson, that they are not terrorists and are erroneously on such lists?

Answer: The Transportation Security Administration (TSA) has established the following procedure to assist individuals who believe that they are improperly included in the No Fly List and Selectee List – collectively known as the TSA Watchlist.

Who may apply for help from this process?

This process only applies to a person who has been delayed as a result of the No Fly List and Selectee List clearance procedures when checking in for a boarding pass for scheduled commercial or charter flights.

NOTE: This process does not apply to persons who undergo enhanced screening at airport security checkpoints.

Who to contact:

TSA, Office of the Ombudsman, at any one of the following:

Office of the Ombudsman
TSA Headquarters
601 South 12th Street – West Tower, TSA-22
Arlington, VA 22202

Toll-free: (866) 289-9673

Email: TSA-ContactCenter@dhs.gov or by clicking on the "Contact Us" button at www.tsa.gov.

How the process works:

- A person may contact the Office of the Ombudsman if that person has been delayed when checking in for a boarding pass due to the No Fly List and Selectee List clearance procedures.
- The Office of the Ombudsman will ask the person to explain their experience to determine what assistance may be provided. If the Office of the Ombudsman confirms that the person's experience is of a type that can be addressed through established procedures, TSA will send a Passenger Identity Verification Form to that person for completion and return.

- TSA requests that the person submit a completed, signed, and dated Passenger Identity Verification Form to TSA providing information to confirming his or her identity and acknowledging: (i) a Privacy Act notice that explains the purpose and routine use of the information provided by the person; and (ii) a statement attesting to the truthfulness of the information and the understanding that knowingly and willfully making any materially false statement, or omission of a material fact, can be punished by fine, imprisonment, or both pursuant to 18 USC § 1001.
- TSA will review the submission and determine whether the Expedited No-Fly List and Selectee List clearance procedures may assist the person's check-in process for a boarding pass.
- TSA will notify the person in writing of its finding. The purpose of this letter is solely to provide a record of the resolution of the passengers' question regarding the Watchlist.
- If the Expedited No Fly List and Selectee List clearance procedures will assist the person's check-in process, TSA will contact the appropriate parties, such as the airlines, to help streamline this process. While TSA cannot ensure that these clearance procedures will relieve all delays, it should facilitate a more efficient check-in process.

6. The Department of Homeland Security has initiated programs and policies to increase security in our air transportation system. For instance, flight cockpit doors have been replaced with reinforced ones, air marshals have been placed on an increased number of domestic flights, pilots may carry firearms, all checked bags are screened, and passengers face a more rigorous screening process. Despite these improvements, the recent downing of two commercial airliners in Russia highlights the continued threat to aircraft, especially international flights.

    a. What added security measures have been required of international air carriers who fly into the United States from abroad?

    b. If a foreign country's screening processes, for either luggage or people, are less rigorous than those of the United States, what additional procedures does the Department require before flights from such a country may enter the United States?

    Combined Answer for a. and b.: TSA recognizes that transportation security is a global issue that requires international collaboration and sharing to strengthen our transportation systems against acts of terrorism and that TSA's responsibilities do not stop at our borders. TSA has a number of mechanisms through which it collaborates and cooperates with the International Civil Aviation Organization (ICAO) and the civil aviation authorities of other nations to ensure that all flights entering the United States are in compliance with relevant international and United States requirements.

    One of TSA's major international initiatives is the Transportation Security Administration Representative (TSAR) Program, which was initiated by the Federal Aviation Administration in 1990 as a result of the destruction of Pan Am

flight 103. The TSA Representative positions were established to promote alignment and consistency between the security requirements of the U.S. and foreign governments and to foster reciprocal relationships with host countries to ensure the security of the air transportation system. The TSARs also have responsibility for ensuring that U.S. and foreign air carriers are meeting U.S. and international requirements for flights to the United States.

TSA's International Aviation Security Specialists are organized in assessment teams that conduct security assessments at all international airports from which U.S. and foreign air carriers provide service to the United States. During Fiscal Year 2004, TSA inspectors and TSARs visited nearly 200 airports around the world. The types of airports assessed include:

- Airports served by U.S. air carriers;
- Airports from which a foreign airline serves the U.S.;
- Airports that pose a high risk of introducing danger to international travel; and
- Other airports considered appropriate by the Secretary of Homeland Security.

The assessment teams use the minimum Standards and Recommended Practices (SARPs) established by ICAO's Annex 17 as a reference of measurement. The primary operational areas of observation during assessment visits are the screening of passengers, carry-on items, and checked baggage; access control measures; cargo screening; and current national security procedures and programs. The assessment teams work to ensure that critical areas of non-compliance are corrected. If compliance cannot be readily obtained, additional measures are immediately placed on the air carriers to counter the critical weakness observed.

TSA has initiated a versatile and near real-time crew vetting system, under which crew members on flights to, from and overflying the U.S. are vetted against a pre-cleared master crew list to identify and deny entry to those persons who pose a potential threat to the United States. To ensure the accuracy and comprehensiveness of the master list, TSA works with foreign governments regarding the exchange of potential threat information to ensure the proper identification of individuals who may pose a threat to transportation security. On March 30, 2004, TSA expanded the scope of crew member vetting to include all persons on all-cargo flights.

Additionally, TSA has deployed personnel to locations such as Istanbul and Moscow to serve as advisors and facilitators for enhanced security in response to actual attacks.

c. Do air marshals, either United States or foreign, fly on all international flights arriving in the United States? If not, can you explain what percentage of such flights includes air marshals?

Answer: The answer to this question is classified and cannot be included in this unclassified document. We would be more than happy to arrange a secure means of providing the Senator with the answer.

What has the Department done to ensure that American pilots may carry their firearms on international flights?

Answer: TSA has opened a dialogue with the Department of State to explore the possibility of expanding the Federal Flight Deck Officer (FFDO) program to U.S. international flights. While the Arming Pilots Against Terrorism Act states that TSA, in consultation with the Secretary of State, "may take such action as may be necessary to ensure that a FFDO may carry a firearm in a foreign country whenever necessary to participate in the program," foreign governments have ultimate authority to authorize U.S. pilots to carry weapons into their sovereign territory.

TSA is currently working with Department of State to determine which countries would be receptive to the FFDO program. Preliminary discussions with foreign governments have not revealed many countries that are interested in allowing armed U.S. pilots into their countries. Firearms are explicitly prohibited in many countries, and U.S. pilots would be subject to countries' firearms laws, which are often strict. If foreign governments were to agree to allow armed U.S. pilots into their territory, crucial issues, such as liability, sovereign immunity, legislation, and logistics would need to be raised and negotiated. At present, TSA does not have an indemnification policy that would compensate an FFDO for an adverse judgment issued by a foreign court for damage to property, personal injury, or death to a foreign national arising from an alleged negligent act.

Senate Judiciary Committee
"The 9-11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security"
Written Follow-Up Questions for The Honorable Asa Hutchinson, Under Secretary, Department of Homeland Security
August 19, 2004

1. Mr. Hutchinson, I asked you at the hearing about the $35 million which was allocatedby Congress in the PY 03 Supplemental Budget bill to be used to issue grants to implement a radiological defense system. The Supplemental money was allocated to DHS on May 14, 2003. Could you please explain why this $35 million has not been spent?

   Answer: These funds have been awarded by the Department of Homeland Security's Office for Domestic Preparedness (ODP). In fact, awards under this program were made on December 30, 2003 under the Urban Areas Security Initiative Radiological Dispersal Device Protective Measures Program. Please see accompanying chart for a breakdown of the awards made on this program and the recipients of those awards.

   The grant award process has been completed and all funds obligated to the NYNJ and Charleston, SC metropolitan areas. Detailed budgets have been developed by the grantees. These budgets have been reviewed and approved by DHS, and resources have now been released to the appropriate agencies within the two regions for the acquisition of radiological sensors and other related equipment, as well as for the development of an integrated approach to response and interdiction relative to an IND/RDD threat.

   It should be noted that $1.1 million of the appropriated amount was dedicated to two key projects that supported the overall goals and objectives of the RDD Program, including an analysis of regional RDD detection and response capabilities and an analysis of regional "choke points" with respect to implementation of RDD systems. Additionally, a portion of the $1.1 million was dedicated to support regional meeting and analyses of the overall results of the pilot projects in New York and Charleston.

State	FY03 UASI Radiological Dispersal Device Protective Measures Program (RDDPMP)		
	Application Submitted	Award Date	Award Amou
New York City Metropolitan Area			$29
New York State Division of Criminal Justice Services	11/25/03	12/30/2003	$7
New Jersey Department of Law and Public Safety	12/02/03	12/30/2003	$7
New York City Office of Management and Budget	11/25/03	12/30/2003	$10
Port Authority of New York and New Jersey	11/24/03	12/30/2003	$
South Carolina Research Authority			$4
National Law Enforcement and Corrections Technology Center – Southeast	11/18/03	12/30/2003	$4

2. If this money has been spent, please tell me how much of this *$35* million has been spent, when it has been spent and for what purposes? Please provide as much detail as possible about how the money has been spent, including detailing the amounts of any grants or disbursements, the recipients, what the money is to be used for and how that spending is related to providing the United States with a radiological defense system. If any of the $35 million has been spent for any other purpose, please provide detailed information concerning that spending as well.

Answer: Grantees in the New York/New Jersey and Charleston, South Carolina are currently in the process of developing plans and ordering radiation detectors and other related equipment in support of this project. For the New York/ New Jersey metropolitan area, the grantees are: the City of New York, the State of New York, the State of New Jersey and the Port Authority of New York and New Jersey. Total funding provided in support of the New York/ New Jersey portion of the project is $30 million. The South Carolina Research Authority serves as the grantee for the Charleston, SC portion of the project. A total of $5 million has been provided in support of this effort. The attached spreadsheets detail the intended use of funds by each grantee.

To date, both regional efforts have succeeded in developing an integrated working relationship with all responsible federal, state, and local agencies to design and implement a "defense in depth" approach to interdicting illicit radiological material. DHS has succeeded in developing a list of radiation detection and response equipment that is commercially available, "state of the art" and that supports a regional approach to radiological detection and interdiction. We have also leveraged our resources by

integrating the efforts of DHS S&T relative to their radiological test beds, as well as the grant, training and exercise capabilities of the Office for Domestic Preparedness, the Transportation Security Administration's multi-modal security initiatives, the DHS Wireless Management Office's IWN program and the activities of other departments and agencies, including DOE/NNSA and the NRC. All resources have been directed to the interdiction of illicit radiological material in the two regions.

3. How much money has DHS requested over the past several years from Congress for nuclear detection devices, how much money has it received and how has that money been used?

   Answer: Requests for the deployment for nuclear detection devices within DHS have been made through the operational Directorates. In FY03 and FY04, $210 million was allocated to Customs and Border Protection (CBP) for the Radiation Portal Monitor program. In FY05, $80 million was allocated to CBP for the procurement of additional radiation portals. As well, funding was allocated to the U.S. Coast Guard for the procurement of portable radiation search devices. The U.S. Coast Guard has deployed approximately 1500 portable radiation detection devices. In addition, grant programs such as the State Homeland Security Grant Program and the Urban Area Security Initiative have supported the acquisition of $14,393,334 million in rad/nuke detection equipment in FY04 alone.

4. Based on information provided by experts in this area, I initially attempted to secure $150 million in FY 03 to implement a radiological defense system for our ports, which experts said would fund the first year of such a program. Does DHS agree that this amount of money is needed to fund the first year of such a program? If not, how much money does DHS believe is needed, What has DHS done, or is DHS doing, to obtain that money from Congress?

   Answer: It is essential that deployments of detection systems components be conducted within a national domestic radiological and nuclear countermeasures system architecture. Deployment of radiation detection equipment at our ports of entry is certainly an essential component of the national countermeasures system architecture and has been occurring over the last two years. In FY03, FY04, and FY05 a total of $290 million was allocated to this activity. DHS believes that the deployment of a radiological defense system to cover all our ports of entry is required and should be completed within the next several years. To date, DHS has requested additional funding for this purpose and has also requested funding for other essential components of the national architecture.

5. Experts have indicated that, for a price tag of $1 billion, America could tighten its borders by installing devices that could detect nuclear weapons as terrorists attempt to smuggle them into the United States, Does DHS agree with this assessment? If not, why not. If so, what is DHS doing to obtain this money from Congress or to otherwise provide for the purchase and installation of devices that can detect nuclear weapons at our ports, our border and in our cities?

   Answer: Deployment of radiation detection equipment at our borders, both at the ports of entry and between the ports of entry (POEs), is certainly an essential component of the

national radiological and nuclear countermeasures system architecture and has been occurring over the last two years. DHS believes that the deployment of a radiological defense system to cover all POEs, the deployment of capability to detect all entries between the POEs, and detection of threats as they are being transported to and within cities that have high potential as targets, are required and should be completed within the coming years. To date, DHS has requested the funding required for the continuing deployment of these essential components of the national architecture.

QUESTIONS FROM SENATOR PATRICK LEAHY

FOR ASA HUTCHINSON, UNDER SECRETARY, DHS

1. We have all heard about major weaknesses in the current watch lists, including the duplication of names and the listing of common names. Instead of narrowing down the targets that pose a significant threat, the lists grow to include thousands of names with no obvious way to discern who should be on the list and who should not This result is an endless pursuit of innocent people -- a waste of time, energy and valuable resources. For example, a recent *Washington Post* article entitled "You, Too, Could Be A Suspected Terrorist" illustrates this problem clearly. The name "Antonio Romero" appears on a U.S. Treasury Department list tilled "Specially Designed Nationals and Blocked Persons." An Internet search found no fewer than 10 "Antonio Romero" names in the New York area alone, How does TSA plan to address these issues as it attempts to expand the "no fly" and "automatic selectee" lists?

   Answer: TSA has consolidated its Watchlist operations (including the No Fly and Selectee Lists) within the Terrorist Screening Center (TSC). This consolidation was done in accordance with the requirements of: 1) HSPD-6, which requires the integration of all the Federal Government's terrorist watch lists and 2) HSPD-11 which requires the implementation of a coordinated and comprehensive approach to terrorist-related screening to support homeland security at home and abroad. TSA is actively working with our federal partners, which include the National Counterterrorism Center (NCTC), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and others to ensure that the TSA Watchlist is as accurate and complete as possible. A key component of the Department's efforts in this area is the expansion of information technology capabilities and links between TSA and the TSC.

   In cases where individuals believe that they are improperly included in TSA Watchlist despite the precautions built into the system, TSA operates a redress process to review their situation and to offer assistance through its clearance procedure to facilitate future travel as appropriate.

2. The Homeland Security Act gave DHS the authority to establish visa policy, and authorized DHS to place employees at diplomatic and consular posts in order to protect homeland security interests.

   a. At how many of our consulates abroad are DHS personnel currently stationed?

      Answer: The Department and its component agencies have numerous personnel serving in diplomatic posts around the world. In addition, the Department has ICE's Visa Security Unit, established in response to section 428 of the Homeland Security Act of 2002. VSU currently has DHS law enforcement officers stationed at two diplomatic posts overseas: Riyadh and Jeddah in the Kingdom of Saudi Arabia. VSU has identified additional locations for DHS officer deployment under this program and is working with the Department of State to deploy these

officers in the near future.

Please note, information concerning the number of DHS officers deployed and their location is considered law enforcement sensitive and should be protected from public disclosure.

b. What are the responsibilities of those personnel?

Answer: DHS personnel serving in this program are known as Visa Security Officers, or VSOs. Section 428 of the Homeland Security Act specifically provides that VSOs will –

- Provide expert advice and training to consular officers regarding specific security threats relating to the adjudication of individual visa applications or classes of applications.
- Review any such applications, either on the initiative of the employee of the Department or upon request by a consular officer or other person charged with adjudicating such applications.
- Conduct investigations with respect to consular matters under the jurisdiction of the Secretary.

In the context of visa security review, VSOs perform a unique review function separate from the consular adjudication process. To do so, VSOs contribute a wealth of law enforcement expertise to the post, including knowledge of immigration law, counter terrorism, document analysis, security threats, intelligence gathering, information-sharing, investigations, interviewing, and fraud detection. An MOU between State and DHS on implementation of Section 428 provides that the "expert advice and training" referred to above includes but is not limited to –

- Gathering and reviewing intelligence reports and coordinating with other agencies at post to consolidate up-to-date information with respect to terrorist or other entities or individuals in the host country who pose a threat to homeland security; determining connections with individuals and groups in other countries which may also constitute a threat; and making this information available to consular officers in a timely and useful manner.
- Briefing consular officers and providing them with training, as appropriate, concerning terrorist or other entities that pose a threat to homeland security and assisting with questions and interview techniques useful in detecting persons who may be a threat or whose applications may be fraudulent.
- Consulting with consular officers on particular visa applicants who raise homeland security concerns.

c. Do they have expertise in recognizing fraudulent passports?

Answer: VSOs have experience detecting fraudulent passports, as well as a variety of other immigration law enforcement skills. All have been trained in fraudulent document detection, both through their initial law enforcement

academy training, and in pre-deployment training specific to their assignment overseas. More importantly, VSOs are experienced law enforcement officers who have cultivated their expertise through years of experience in a variety of enforcement professions, including as special agents, inspectors at ports of entry, Border Patrol agents, and deportation officers. This provides a depth of expertise that training alone can neither provide nor replace. VSOs also have access to additional resources and expertise, such as the ICE Forensic Document Laboratory, to assist them in their work.

3. The Commission Report places great emphasis on building on the success of the Government's small terrorist travel intelligence collection and analysis program, and says that "constraining terrorist travel should become a vital part of counterterrorism strategy."

   a. Should ICE have its own unit that works specifically on terrorist travel issues?

      Answer: ICE does currently have a unit within the National Security Investigations Division that focuses specifically on the entry and exit of all travelers to and from the United States. ICE created the Compliance Enforcement Unit (CEU) in June 2003 to investigate suspected violations reported from a range of immigration registration systems implemented after 9/11, including the Student Exchange Visitor Information System (SEVIS), the National Security Entry Exit Registration System (NSEERS) and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT). These databases provide the U.S. Government with a means to track and pursue foreign students, exchange visitors and other non-immigrants who violate their immigration status - capabilities that did not exist before 9/11. The CEU further developed and staffed the Threat Analysis Section (TAS) that was developed to support a more targeted NSEERS interview process to replace the mandatory 30-day/1-year interviews.

      The National Security Investigations Division has further increased ICE's presence four-fold at the Customs and Border Protection (CBP) National Targeting Center (NTC). This increase of ICE presence has allowed ICE to be operationally responsive twenty-four hours a day, seven days a week to CBP terrorist related TIPOFF contacts and other issues at U.S. Ports of Entry. In addition, the National Counterterrorism Center will submit to Congress, in accordance with Section 7201 of the Intelligence Reform and Terrorism Prevention Act of 2004, a strategy for addressing terrorist travel.

   b. Will DHS follow the Commission's recommendation to ensure that information systems that can authenticate travel documents and detect potential terrorist indicators are in use at consulates, primary border inspection lines, immigration services offices, and intelligence and enforcement units?

      Answer: CBP is working closely with US-VISIT and the International Civil Aviation Organization (ICAO) to conduct mock testing of document readers capable of reading and authenticating electronic passports (e-Passports), which Visa Waiver Countries must have in place by October 26, 2005. In addition CBP continues to work with US-VISIT to integrate systems with the Department of

State and other DHS agencies to authenticate both U.S. and foreign travel documents. DHS, through US-VISIT (Office of Screening Coordination), will also explore and implement the recommendations contained within the HSPD-11 report; which includes a full coordination of terrorist screening efforts and practices government-wide.

c. What training will be provided to DHS personnel on terrorist travel habits?

Answer: The Federal Law Enforcement Training Center (FLETC) has provided counterterrorism training for more than a decade. Currently, the FLETC offers and conducts training on criminal information/intelligence gathering in the basic training programs provided to our 81 Partner Organizations. Acknowledging that intelligence or information gathering is the responsibility of all law enforcement personnel and in response to the expanding missions in the post September 11, 2001 environment, the FLETC is taking the initiative to provide training in the area of recognition of pre-incident indicators of a terrorist attack.

Pre-incident indicators will exist for each terrorist attack, domestic or international. Some of the indicators are identification cards and passports (indicators including the travel habits of terrorists), maps and blueprints, GPS, components of manned portable air defense systems (MANPADS) or weapons, literature of an extremist nature, posters, flags, and the behavior of the suspected terrorist. Law enforcement officers must be able to recognize and report the suspicious activities and behavior of suspected terrorists. Pre-incident indicators, viewed individually, can escape meaning but when properly collected and analyzed against known methods of operation, they may forecast an incident, identify an individual, or show a group in their logistical preparation. The FLETC has developed and is currently implementing training on the collection of pre-incident indicators that will prepare the students for their expanded role in the fight against terrorism. In addition, training will be provided in the form of practical exercises to expose the students to the indicators in real world situations.

The initial class was piloted to a Mixed Basic Police Training Program on October 25, 2004. This pilot included a two-hour presentation on pre-incident indicators within the first four days of training. During this training, some pre-incident indicators were presented during some training, labs, and practical exercises. Students had to recognize these indicators and report them to a central phone number furnished by the Counter Terrorism Division. Another two hour class were held during their 5th week to ensure the students had no questions about the pre-incident indicators that were present during the first 5 weeks of their program. A final debrief on the pre-incident indicators was presented to the students in their last week of training. To enhance the training experience, classes on Terrorism, MANPADS, Bombs and Explosives, and Weapons of Mass Destruction was elevated to earlier time slots during the training schedule. Students were required to recognize the pre-incident indicators without help from the supervisory instructor. This made the mid-point review and final debrief more relevant.

Additionally, a video with different vignettes depicting pre-incident indicators and a pocket sized spiral bound reference guide for the students has been prepared and was available for students to take back to their ports of duty. It is estimated that upwards of 10,000 trainees will be exposed to this training over the next few years; however, that number could be expanded.

4. The Report states that fraudulent travel documents are usually returned to travelers who are denied entry to the United States, I know that this has been a concern of Senator Feinstein. Will DHS adopt a policy of confiscating fraudulent travel documents?

Answer: With regard to the disposition of fraudulent documents encountered at ports of entry, DHS is committed to removing these documents from circulation. Under current practice, if the alien is not immediately removed from the United States, the document either remains with the casework or, in particular cases, be forwarded to the Forensic Document Laboratory (FDL) for evaluation, etc. Whenever possible, the document is retained and the alien removed from the United States either on photocopies of the documents, the International Civil Aviation Organization (ICAO) agreed letter, or without a travel document, if the country of departure to the United States will accept him. In certain cases, particularly when the country of embarkation is reluctant to accept back an individual without a travel document or when extended detention has been involved, efforts may be made to obtain a legitimate travel document from the appropriate foreign authorities. In some of these cases, it has been necessary to "return" the passport so that the individual can been returned to the point of embarkation. In these cases, the document is given to the airline representative who is supposed to turn it over to the authorities in the country of departure. Unfortunately, we believe that airline practices vary greatly, both between airlines and airports and, in some cases, the documents may have been returned to the individual rather than to the appropriate officials.

However, DHS is establishing a policy aimed to prevent the return of fraudulent documents to the alien and eliminate the potential for reuse. Consistent with this goal, the Bureau of Customs and Border Protection is currently developing updated, specific guidance to the ports for the handling of fraudulent documents to prevent the re-entry of the document into circulation.

5. The Report recommends that in conjunction with steps that should be taken to harden our borders, programs to speed known travelers across our borders should be a higher priority. It also recommends the consolidation of a number of existing such programs. How will DHS respond to those recommendations?

Answer: DHS is working to consolidate all registered traveler programs into one initiative in accordance with the 9-11 Commission recommendation. Customs and Border Protection (CBP) in conjunction with the Canada Border Services Agency (CBSA) and Citizenship and Immigration Services (CIS)has developed and implemented NEXUS Air pilot Project. The pilot facilitates passage into Canada and the United States for pre-approved, low-risk, frequent air travelers using automated

kiosks with iris-recognition biometric technology. NEXUS Air arises from the 2001 Canada-United States Smart Border Declaration commitment to improve the secure flow of people and goods between the two countries.

Customs and Border Protection is working in conjunction with USVISIT and the Department of Homeland Security to develop a Passenger Accelerated Service System (CBP-PASS, this is the working title and could be changed in the future) to provide a replacement for the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) and to implement a single integrated passenger processing system that will expedite the movement of international low-risk, frequent air travelers by providing an alternative primary inspection process for pre-approved, pre-screened eligible travelers.

By implementing this initiative CBP will make great strides toward facilitating the movement of people in a more efficient manner thereby accomplishing our strategic goal of balancing legitimate trade and travel with security. Additionally, DHS will be addressing the recommendation made in the 911 Commission Report that states "The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers. It should be integrated with the system that provides benefits to foreigners seeking to stay in the United States."

6. DHS recently announced a new passenger screening program, *Secure Flight,* which will screen passengers against a compiled watch list created by the Terrorist Screening Center.

    a. Given that the implementation of this program will take some time, in the interim, against which databases will the names of airline passenger manifests be checked? What databases are currently used for checking manifests?

    Answer: Pending the development and full implementation of Secure Flight, domestic and foreign air carriers who fly into, out of, or through U.S. airspace will continue to check their passenger name lists against the No-Fly and Selectee Lists (collectively referred to as the TSA Watchlist Program) maintained by the Terrorist Screening Center (TSC) with TSA assistance.

    b. As the recent experiences of Senator Kennedy and Representative John Lewis show, there are significant weaknesses in the watch lists in terms of accurate identification of potential terrorists, and the success of any screening program will depend on data quality. What actions does DHS plan to take to ensure that the watch lists used to implement the current and future screening programs are as accurate, useful and as complete as possible?

    Answer: TSA has consolidated its Watchlist operations (including the No Fly and Selectee Lists) within the Terrorist Screening Center (TSC). This consolidation was done in accordance with the requirements of: 1) HSPD-6, which requires the integration of all the Federal Government's terrorist watch lists and 2) HSPD-11 which requires the implementation of a coordinated and

comprehensive approach to terrorist-related screening to support homeland security at home and abroad. TSA is actively working with our federal partners, which include the National Counterterrorism Center (NCTC), the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and others to ensure that the TSA Watchlist is as accurate and complete as possible. A key component of the Department's efforts in this area is the expansion of information technology capabilities and links between TSA and the TSC.

7. The Report recommends a biometric entry-exit screening program, and in particular suggests that a solution to allow speedy passage for qualified travelers may be a combination of radio frequency technology and biometric identifiers. Earlier this summer, the Department launched pilots of its "Registered Travelers" program which would allow qualified travelers to avoid delays by using "smart cards" containing chips embedded with biometric information.

   a. What are the results of the "Registered Travelers" pilot program, and when does the Department plan to implement this program nationwide?

      Answer: The mission of the Registered Traveler (RT) Pilot Program is to introduce biometric technology – such as fingerprints, digital photographs, and iris scan technology – in conjunction with prescreening security assessments and to test possibilities for expedited screening procedures (e.g., use of dedicated lanes) at airports for qualified individuals. The RT Pilot Program is voluntary, and there is currently no fee associated with participation.

      Over summer 2004, TSA launched RT pilots at five airports nationwide in partnership with major air carriers. TSA is working with Northwest at Minneapolis, United at LAX, Continental at Houston, and American at Boston and Reagan National. Each site is conducted as a stand-alone project. TSA is in the process of analyzing the results of these pilots.

      TSA has extended the five pilots through September 2005 to test interoperability and to begin the development of a technical infrastructure. In addition, TSA will explore a business model for a public/private partnership that is planned to launch as a new pilot at Orlando in 2005.

   b. What is the Department's assessment of the timeframe and costs for deploying hardware and software infrastructure for this program, and will this infrastructure be compatible with other government biometric entry-exit screening programs?

      Answer: TSA is in the process of analyzing information from the five RT pilots. The Department will use these results to determine the feasibility of expanding the Registered Traveler program.

c. Has the Department evaluated the privacy challenges associated with using biometric and other personal information for this program, and what procedures and mechanisms are in place to protect traveler privacy?

Answer: DHS and TSA are cognizant of the importance of safeguarding the personal information of travelers, especially when handling biometrics given the concern of identity theft and fraud. TSA has analyzed the privacy risks associated with the collection of biometric identifiers. TSA has also examined the types of mitigation measures prior to implementing the pilot phase of RT to ensure that biometric information will be secure. As a result, TSA has taken every reasonable precaution to secure biometrics collected for the purpose of the RT pilot, including strictly limiting access by TSA personnel to the data in order to ensure individual privacy is being protected.

The public has been notified of the Department's privacy safeguards for the Registered Traveler Pilot Program through the publication of the RT Privacy Impact Assessment (PIA), which was posted to the DHS website on June 24, 2004. DHS welcomes feedback on the PIA; as of December 2004, no comments have been received.

A RT participant's biometric identifier may be stored in two places: 1) on the individual's RT card where it is encrypted and encoded; and 2) in the RT database located where the pilot is taking place. RT databases are secured in accordance with the Federal Information Security Management Act of 2002, (Public Law 107-347), which established government-wide computer security and training standards for all persons associated with the management and operation of federal computer systems.

In addition to meeting the federal standard for securing data, TSA has instituted extra security measures to protect all personally identifiable information, including biometrics. The enhanced security measures include the following technical safeguards to secure data:

- Use of advanced encryption technology to prevent internal and external tampering of data and transmissions;
- Secure data transmission including the use of password-protected e-mail for sending files between the security threat assessment participants to prevent unauthorized internal and external access;
- Password protection for files containing personal or security threat assessment data to prevent unauthorized internal and external access;
- Network firewalls to prevent intrusion into DHS network and TSA databases;
- User identification and password authentication to prevent access to security threat assessment systems by unauthorized users; and

- Security auditing tools to identify the source of failed TSA system access attempts by unauthorized users and the improper use of data by authorized operators.

These security measures are designed to protect individual privacy and prevent against identity theft. As new technologies emerge, TSA continues to examine whether and how they might further enhance personal privacy and security of personal information.

8. The U.S. is currently participating in the process before the International Civil Aviation Organization to establish technical standards for biometric passports. Given that these standards will be a basis for U.S passports, it is likely that the ICAO conclusions will impact domestic biometric programs, What, if any, measures has the Department taken to guide the ICAO process to assure that the final standards ICAO promulgates are decided in an open manner so that Congress and the public can ensure the protection of privacy and civil liberties.

Answer: The use of biometrics in a security context raises important questions and concerns related to the protection of privacy and personal data. As a result of this, representatives from the United States Government, including the Department of State and the Department of Homeland Security (DHS), have been actively involved with ICAO and other organizations, such as the International Standards Organization (ISO), to ensure that, if international standards are developed, they take into account the particular concerns of the United States regarding privacy and civil liberties in a security setting. The United States is committed to participating in an open and transparent way with international organizations on the use of biometrics for travel documents and will press its concerns at every opportunity.

9. The Department recently awarded a contract to Accenture to implement the next generation of the US-VISIT program, which currently collects biometric information from travelers. US VISIT will also include travelers from Visa Waiver countries who will be using biometric passports.

   a. Has the Department given Accenture directives in addressing the privacy and data security issues connected with the use of biometric information? Please provide any documentation associated with these directives.

   Answer: As part of any application development activity, including biometrics, the Accenture integrator as well as any other DHS contractor supporting US-VISIT functionality is being overseen by the US-VISIT Chief Information Officer and is following a System Development Life-Cycle (SDLC). As part of that SDLC, information security is a key component, and furthermore US-VISIT has instituted a concurring signature at each SDLC gateway review by the US-VISIT Privacy Officer. Finally, the US-VISIT Privacy Officer oversees and conducts Privacy Impact Assessments (PIAs) and ensures that technology systems and system owners adhere to and update System of Record Notices (SORNs) and other OMB and regulatory and legislative guidance as to privacy and information security.

b. Will the technology and information infrastructure created by Accenture be expandable beyond the US-VISIT program to include or be compatible with a broader biometric entry-exit screening program or any other government security initiatives that include data gathering?

Answer: Yes. US-VISIT will continue to follow, be informed by, and influence as appropriate, the DHS Enterprise Architecture and Technical Reference Model. The US-VISIT future target technical approach and platform will be open architecture, component based, and scalable. To date, the success of US-VISIT delivery and real mission capability has been accomplished through integration, interoperability, and modernization of systems and infrastructure.

10. On April 8, 2004, the Subcommittee on Terrorism, Technology and Homeland Security of the Judiciary Committee held a hearing on "Keeping America's Mass Transportation System Safe: Are the laws adequate?" At that time, Gary Bald, Acting Assistant Director, FBI, deferred to the "Administration" and the Department of Homeland Security regarding the following question.

"In his testimony, Mr. Bald makes a strong case that U.S. ports, which are run by state and local authorities, are critical to the nation's economy but are inherently vulnerable and an attractive target for terrorists. He also states that "one significant challenge is the limited amount of funding and resources available to the state and local agencies, including the port authorities, to address the many issues involved in securing our ports from terrorist attacks." According to U.S. Coast Guard estimates, ports will need to spend *$5.4* billion over the next ten years on infrastructure and personnel to comply with new federal regulations mandated by the Maritime Transportation Security Act (MTSA) ($ 1.125 billion just in the first year). (A) If ports are a national security priority, why hasn't the Administration done more to seek and provide financial assistance for these state and local government entities? (B) Specifically, why did President Bush not seek funding for port security grant funding in his proposed budgets for Fiscal Years 2003 or 2004? (C) Despite President Bush's decision not to seek such funding, should Congress have provided more generous funding for port security grants than it has?"

Would you please provide the answer?

Answer (A):

Like most other homeland security efforts, improved port security is a shared responsibility of Federal, State, and local governments, as well as the private sector. DHS continues to make significant investments in port security through the Coast Guard and Customs and Border Protection. While the Coast Guard did provide an estimated of the compliance costs of MTSA, this is an established part of the drafting and review of Federal regulations, and does not imply that the Federal government is responsible for reimbursing these costs.

DHS does recognize that ports are one of the many homeland security priorities faced by State and local governments. The Department of Homeland Security Appropriations Act for Fiscal Year (FY) 2005 includes more than $3.9 billion to

support State and local homeland security efforts. The DHS Appropriations Act includes funds to continue the Homeland Security Grant Program (HSGP), which includes the State Homeland Security Program at $1.1 billion; the Law Enforcement Terrorism Prevention Program at $400 million; and the Citizen Corps Program at $15 million. Funds are also provided for the continuation of the Urban Areas Security Initiative (UASI) at $885 million.

Under both the HSGP program and UASI program, States, localities, and urban areas are eligible to use their HSGP and UASI funds to purchase physical security enhancement equipment (otherwise known as "target hardening" equipment). Among the allowable expenses under this category, which is outlined in the program guidance for both HSGP and UASI, are: motion detector systems, barriers, impact resistant doors and gates, video and radar systems, and chemical agent and explosives detection equipment. All of these types of equipment can be used to secure a number of different critical infrastructures, including port facilities.

Under these programs, the Department permits States and localities, considerable discretion in the distribution of their homeland security funds. Through the State Homeland Security Assessment and Strategy Process, which both States and urban areas must conduct to receive their HSGP and UASI funds, respectively, States and urban areas are given the necessary tools to determine needs and vulnerabilities and, in turn, make informed decisions on the most effective means to use their homeland security funds. If they chose, States and urban areas could use their funds to target harden ports and port facilities. This is a decision, however, that States and urban areas must determine through their assessment and homeland security strategy process, and through continued consideration of threats and risks.

Answer (B): In FY 2003, ODP administered the State Homeland Security Grant Program (SHSGP), Part I and II. Under both of these programs states, territories, and the District of Columbia (DC) are allowed to use their allocated funds to purchase equipment that could be used for target hardening of critical infrastructure sites, including port facilities. ODP provided significant funds under SHSGP, Part I and II. Under Part I, ODP provided $500 million for states, territories and DC, to purchase equipment, and support training, exercise, and planning activities. Under Part II, ODP provided $1.3 billion for the same purpose areas.

Additionally, in FY 2003, ODP administered UASI Part I and Part II. Under these two programs, ODP provided $800 million for an initial 30 high threat, high density urban areas, including $75 million dedicated to port security efforts. States and urban areas determined how to distribute their funds on comprehensive needs, vulnerabilities, threats, and capabilities assessment, and the development of a homeland domestic preparedness strategy. As with SHSGP funds, urban areas could use their UASI funds to enhance security at critical infrastructure sites, including port facilities.

Answer (C): As discussed above, the FY05 Budget request included port security as one of many eligible activities within the $3.6 billion request for the Office of Domestic Preparedness, through $46 million was specifically requested for port security exercises. The FY05 appropriation did provide $150 million for port security grants, which will be awarded by ODP in cooperation with TSA and the Coast Guard.

SENATOR LEAHY QUESTIONS

(a) *One issue you raised in your written statement caused me great concern. Specifically, you have brought to my attention the fact that Amtrak cannot, in some states, like California, directly access law enforcement records systems while performing pedestrian and vehicle investigations. Can you detail what impediments exist such that Amtrak cannot access law enforcement records when necessary to do so for a complete investigation and can you provide suggestions on what can be done to ensure that your officers have access to key and critical law enforcement data?*

Answer: The Department of Homeland Security recommends that the Committee solicit Amtrak's views on this issue. Nonetheless, it is important to note that this issue is not solely an Amtrak Police issue. No Rail Police can access the California Law Enforcement Telecommunications System (CLETS). CLETS provides up to date, local criminal history (warrants, wanted person etc.) and driver information. Thus, it is an important technological data tool for field officers who are conducting pedestrian and vehicle investigations, In 2002, Amtrak Police attempted to clarify this issue and was advised by the California Attorney General's Office that rail police are not eligible to receive this information directly because rail police are not regarded as a "public agency of law enforcement." See California Government Code Sections 15151 and 15153. Basically, only state, local and sheriff's department personnel have a "right" to receive this information directly, even though Amtrak police officers are filly accredited.

However, state summary criminal history information "may" be provided because Amtrak Police demonstrated a "compelling need" as described in California Penal Code 11105(c). This "need" is evaluated on a case-by-case basis. Amtrak and other Rail Police Officers have to call the California Department of Justice (DOJ) Command Center and request the information (as opposed to contacting a California local Police Radio system via radio and making the same request). The request is evaluated to determine if it meets a "compelling need". If there is an issue, the Command Center will then contact the California DOJ Record Security Section for a final determination.

This can create significant officer safety issues because of the length of time that it may take for a response.

Senate Judiciary Committee
Rearing on "The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security"
August 19, 2004

Written Questions Submitted by Senator Russell D. Feingold

Questions to The Honorable Asa Hutchinson

1. The 9/11 Commission recommends that the Department of Homeland Security assume responsibility for the screening of airline passengers against the so-called "no-fly" or terrorist watch lists, a task that is currently performed by the airlines, One of the Commission's concerns is that the government does not share complete information with private entities. On August 16, 2004, you announced that the Department had begun to act on the Commission's recommendation and would assume full authority to screen passengers against the government's full set of terrorist watch lists.

    a. Could you comment further on your plans? What steps has the Department taken, when did they begin, and what is your timeline for full implementation of this recommendation?

    Answer: On September 24, 2004, DHS announced its intent to implement a next generation aviation passenger prescreening program called Secure Flight. Secure Flight will meet the Department's goals of improving the security and safety of travelers on domestic flights, reducing passenger airport screening time, and protecting privacy and civil liberties.

    In the interim, measures are being taken by TSA to improve performance of the current screening conducted by the airlines pending rollout of Secure Flight. These measures include a revision to the CAPPS rules and review of the entries in the current "no-fly" and Selectee lists used by the Airlines for screening, coordinated with Terrorist Screening Center.

    Description

    Under Secure Flight, the Transportation Security Administration (TSA) will take over from the air carriers the comparison of domestic airline Passenger Name Record (PNR) information against terrorist watchlists. Secure Flight will use records contained in the consolidated Terrorist Screening Center Database (TSDB), to include the No-Fly List and Selectee List – collectively known as the TSA Watchlist. TSA anticipates applying a streamlined subset of the existing CAPPS I rule set to PNRs. TSA will also build a "random" element into the new program to protect against reverse engineering by those who would seek to defeat it. The new Secure Flight program will improve the efficiency of the prescreening process and reduce the number of people selected for secondary screening.

This new system carries multiple benefits over the current CAPPS I system. TSA will be able to use the consolidated watch lists contained in the TSDB, including the expanded No Fly and Selectee lists. Consolidating these checks within the Federal Government will allow TSA to automate most watch list comparisons and apply more consistent internal analytical procedures when automated resolution of initial "hits" is not possible. It will help eliminate false positive Watchlist matches that some passengers experience under the existing system and, thereby, helping move passengers through airport screening more quickly, reducing the number of individuals selected for secondary screening, and allowing for more consistent response procedures at airports for those passengers identified as potential matches. Consequently, TSA will be able to concentrate its screening resources more efficiently.

Secure Flight differs from earlier proposed systems by eliminating the predictive "risk assessment" features. It also focuses screening efforts on solely looking for known or suspected terrorists, rather than using the system for other law enforcement purposes.

Under Secure Flight, TSA will only conduct passenger prescreening for domestic flights. This aspect responds to concerns expressed by the aviation community and our international partners about potential duplication of efforts within DHS. Passengers on international flights will continue to be checked against names in the consolidated TSDB by U.S. Customs and Border Protection (CBP), through its Advanced Passenger Information System (APIS). U.S. law mandates that these checks occur.

Civil Liberties and Privacy Rights

To protect passengers' personal information and civil liberties, Secure Flight will:

- Include robust redress mechanisms to enable passengers to work with TSA to resolve instances in which they think they are being inappropriately selected for secondary screening or they are having a difficult time obtaining boarding cards.

- Not consider race or ethnicity as the sole basis for further government action, consistent with the Department of Justice's Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (June 2003). Reliance on generalized stereotypes is forbidden.

- Not use current passenger information for any other purpose than to conduct the watch list comparisons (possible including, depending on the outcome of commercial data test, verification of identity) except in the instances in which positive matches on the TSDB are identified.

As discussed in the response to your next questions, TSA will establish a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening. An appeals process

will be included to allow for review by the TSA Privacy Officer, the DHS Chief Privacy Officer and/or the respective DHS and TSA offices of civil rights.

Testing

On September 21, 2004, TSA announced the release of three documents to enable the testing of Secure Flight. These documents cover TSA statutory authority for activities during the testing phase only.

- A Privacy Impact Assessment (PIA) that explains in detail the handling and flow of personal information and the protocols and privacy protections that are built in to Secure Flight to protect passengers' personal information. The system is designed around a core of privacy statutes, regulations, and DHS policy;

- A System of Records Notice (SORN) that describes TSA's statutory authority to collect data and conduct a test of Secure Flight; and

- An Information Collection Request (ICR) that requests approval from the Office of Management and Budget (OMB) to collect airline PNRs for testing purposes. This document includes the proposed order to all domestic airlines requiring them to provide historic (i.e. completed) PNRs for all passengers who flew in June 2004. OMB has subsequently approved the collection of this data.

The comment period for these documents remained open for 30 days, ending on October 25, 2004.

On November 12, 2004, TSA issued an order for all domestic airlines requiring them to provide historic PNR data that they collected from passengers who flew in the month of June 2004. Records from this period will be used to test the Secure Flight computer platform at full load and speed.

With these significant steps, domestic airlines began the transfer of data in mid-November, allowing testing of Secure Flight to begin in early December 2004. The testing phase is critical to determine system capabilities, capacity and selection rates.

Separately from the testing described above, TSA will also conduct a very limited test to determine whether or not the use of commercial data could assist with identifying passenger information that is incorrect or inaccurate or assist with resolution of false positive matches. TSA will use data that is already commercially available from aggregators. TSA does not assume that commercial data is indicative of passenger intent.

Any testing using commercial data would only occur in accordance with Section 522(d) of the Department of Homeland Security Appropriations Act, 2005 (P.L. 108-334). This provision requires that TSA develop – and the Government

Accountability Office (GAO) evaluate – measures to determine the impact on aviation security by an identity verification system that utilizes at least one database that is obtained from or remains under the control of a non-federal entity. TSA is in the process of developing these measures and providing GAO with necessary information for an evaluation.

Once these criteria are met, TSA's testing of the use of commercial data will be governed by strict privacy and data security protections, including strict prohibitions on the use of any passenger-provided information by commercial data providers. TSA will not incorporate the use of commercial data until testing confirms that:

- It enhances security;
- It does not result in inappropriate differences in treatment of any category of persons; and
- Robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain inappropriate access to or use passengers' personal information inappropriately.

TSA will not make a final decision about incorporating the use of commercial data into the Secure Flight Program prior to the completion of testing, assessment of results, and publication of a new SORN and PIA announcing the use of commercial data and how the privacy of individuals will be protected. Results of the testing, both of the comparisons of PNR information against names in the TSDB and the use of commercial data, will be as publicly transparent as possible without compromising national security. Testing and eventual implementation will be governed by strict privacy protections including passenger redress procedures, data security mechanisms, and limitations on use.

On December 17, 2004, the Intelligence Reform and Terrorism Prevention Act of 2004 became law. Section 4012 sets several milestones and accompanying deadlines for testing of an advanced airline passenger prescreening capability and for the subsequent assumption of that function by the Federal Government. TSA is in the process of complying with these milestones and deadlines.

b. As you know, serious concerns have been raised about the accuracy of "no-fly" lists and other terrorist watch lists. Innocent people have been repeatedly flagged, and some have even had their travel plans delayed or cancelled as a result, There was an incident in Wisconsin two years ago in which several peace activists on their way to Washington for a political demonstration were stopped and interrogated when one member of the group apparently triggered a false positive match on the list. On August 17, 2004, the executive director of the American Civil Liberties Union wrote an op-ed in the *Washington Post* in which he noted that a version of his name, Antonio Romero, appears on a government watch list. This example colorfully illustrates the potential for these watch lists to lead to inconvenience and error. I would like to think that by having the Department

maintain control of screening passengers against watch lists, we will significantly reduce the instances in which innocent people are flagged and stopped. What steps will you and the Department take to ensure that the lists used by TSA and other DHS components are cleaned and scrubbed to include accurate and sufficient information, so that the number of people prevented from boarding a flight or getting a job because their name happens to be similar to another person on a watch list is significantly reduced?

Answer: The Transportation Security Administration (TSA) has established the following procedure to assist individuals who believe that they are improperly included in the No Fly List and Selectee List – collectively known as the TSA Watchlist.

Who may apply for help from this process?

This process only applies to a person who has been delayed as a result of the No Fly List and Selectee List clearance procedures when checking in for a boarding pass for scheduled commercial or charter flights.

NOTE: This process does not apply to persons who undergo enhanced screening at airport security checkpoints.

Who to contact:

TSA, Office of the Ombudsman, at any one of the following:

Office of the Ombudsman
TSA Headquarters
601 South 12th Street – West Tower, TSA-22
Arlington, VA 22202

Toll-free: (866) 289-9673

Email: TSA-ContactCenter@dhs.gov or by clicking on the "Contact Us" button at www.tsa.gov.

How the process works:

- A person may contact the Office of the Ombudsman if that person has been delayed when checking in for a boarding pass due to the No Fly List and Selectee List clearance procedures.

- The Office of the Ombudsman will ask the person to explain their experience to determine what assistance may be provided. If the Office of the Ombudsman confirms that the person's experience is of a type that can be addressed through established procedures, TSA will send a Passenger Identity Verification Form to that person for completion and return.

- TSA requests that the person submit a completed, signed, and dated Passenger Identity Verification Form to TSA providing information to confirming his or her identity and acknowledging: (i) a Privacy Act notice that explains the purpose and routine use of the information provided by the person; and (ii) a statement attesting to the truthfulness of the information and the understanding that knowingly and willfully making any materially false statement, or omission of a material fact, can be punished by fine, imprisonment, or both pursuant to 18 USC § 1001.

- TSA will review the submission and determine whether the Expedited No-Fly List and Selectee List clearance procedures may assist the person's check-in process for a boarding pass.

- TSA will notify the person in writing of its finding. The purpose of this letter is solely to provide a record of the resolution of the passengers' question regarding the Watchlist.

- If the Expedited No Fly List and Selectee List clearance procedures will assist the person's check-in process, TSA will contact the appropriate parties, such as the airlines, to help streamline this process. While TSA cannot ensure that these clearance procedures will relieve all delays, it should facilitate a more efficient check-in process.

2. In its discussion about the need for more effective screening systems at our borders, the Commission advocates "a system for screening, not categorical profiling" and that such a system should look for particular, identifiable suspects or indicators of risk. As you know, last year, the Justice Department issued guidelines to federal law enforcement agencies banning racial profiling.

   a. What steps are you taking to implement the Justice Department's guidelines and the Commission's advice to ensure that DHS officials do not engage in racial, ethnic or religious profiling and instead focus on suspicious behavior and legitimate intelligence or law enforcement leads?

   b. Have you ordered training for DHS officials to ensure that they understand what constitutes racial profiling?

   Answer to a. and b.: The Department of Justice released its Guidance on the Use of Race by Federal Law Enforcement Agencies on June 16, 2003. On June 17, 2003, Secretary Ridge issued a directive that all "appropriate personnel and components review all operations, protocols, policies, guidance and training materials to ensure consistency with [the DOJ] guidance." The DOJ Guidance was promptly circulated to all Departmental elements, and those elements were directed to disseminate the Guidance to all personnel.

   On June 1, 2004, the Secretary issued a directive ordering the inclusion of a short policy statement summarizing the Guidance in all enforcement manuals and any other guidelines covering any activity in which questions regarding the use of race

or ethnicity might arise. The Secretary also directed the DHS Office for Civil Rights and Civil Liberties (CRCL) to promulgate Department-wide training to ensure the Guidance is interpreted and applied in a consistent manner. CRCL worked with the Secret Service's Legal Training Section at the Rowley Training Center, to develop a computer-based, in-service training module which will be made available to all Department personnel, with rollout starting in mid- to late October. CRCL also worked closely with the Federal Law Enforcement Training Center's Legal Training Division to ensure initial entry law enforcement training (which FLETC provides for over 80 federal law enforcement components) is in compliance with the DOJ Guidance.

c. Have you implemented a complaint and disciplinary procedure to deal with alleged instances of racial profiling? If not, will you do so?

Answer: The Department takes allegations of racial or ethnic profiling seriously. Section 705 of the Homeland Security Act, 6 U.S.C. § 345, directs the appointment of an Officer for Civil Rights and Civil Liberties to review and assess allegations of racial or ethnic profiling, as well as other allegations of civil rights or civil liberties abuses by Department personnel. The officer is Daniel W. Sutherland.

In accordance with section 705, the Office for Civil Rights and Civil Liberties is publicizing its existence via a newspaper campaign, an internet presence and with public posters, and inviting public contact by email, telephone, postal mail, fax or TTY. This has allowed the Office to start receiving complaints and comments from the public. After review by the Office of the Inspector General, these complaints are then either retained for review by the CRCL, or forwarded to the appropriate component activity for resolution. Retained complaints are handled by attorneys in the Office of Chief Counsel of the Office for Civil Rights and Civil Liberties. Complaints forwarded to components are monitored to ensure they are resolved by the components in accordance with applicable law and policy. Emphasis is placed on working cooperatively with Department and component leadership to resolve problems, providing proactive policy advice to avoid future shortcomings, and informing the complainant of the review. Because the Officer for Civil Rights and Civil Liberties reports directly to the Secretary, the Office is well positioned to offer policy advice, to resolve specific complaints, and to monitor the complaint resolution process of other DHS components with respect to CRCL's issues, including racial profiling. This organizational framework and these activities are reported in the first annual report of the Office for Civil Rights and Civil Liberties, which was submitted by the Secretary to Congress in May 2004.

In addition to CRCL, several pre-existing offices within DHS Headquarters and components may have some shared or exclusive jurisdiction over complaints relating to civil rights, civil liberties, and racial or ethnic profiling. The extent of their jurisdiction depends on the exact nature of the complaint raised, and investigative authority of the particular office. These offices include the Office of Inspector General, Internal Affairs divisions, Offices of Professionalism or

Customer Service units, and certain component civil rights elements. Depending on the exact nature of a given complaint, these offices may have exclusive jurisdiction, or may share jurisdiction over investigating such complaints. Regardless of how jurisdictional questions are resolved in particular cases, these offices have all worked collaboratively with CRCL to resolve complaints.

With respect to disciplinary systems, the Secretary's June 1, 2004 directive orders the components to hold all personnel accountable for meeting the standards set forth in the DOJ Guidance. Those who violate Department policy or the law will be disciplined in accordance with component procedures. The proposed Human Capital regulations include a number of changes to adverse actions which will streamline the procedures and provide for greater individual accountability.

QUESTIONS FROM CHAIRMAN HATCH
SENATE JUDICIARY COMMITTEE
"THE 9/11 COMMISSION AND RECOMMENDATIONS FOR THE FUTURE OF FEDERAL LAW ENFORCEMENT AND BORDER SECURITY"
AUGUST 19, 2004

Questions for Commissioners Hamilton & Gorton

1. The Commission has counseled against the creation of a new domestic intelligence agency (the so-called "American MI-5"), and has instead called for the creation of an "intelligence cadre" within the Federal Bureau of Investigation ("FBI"). To this end, the Commission has recommended that, after an introductory period of multi-disciplinary training, FBI agents should be allowed to specialize in national security matters for their entire careers.

a. While creating a separate career track for intelligence agents may foster much needed expertise, are you concerned that it may also engender divisions within the FBI workforce or recreate the "wall" between criminal and intelligence investigators?

b. Aside from the multi-disciplinary training of new FBI agents and the intelligence certification of field office deputies, what additional steps, if any, would you recommend to ensure the continued integration of the FBI's criminal, intelligence and counterterrorism missions?

2. The Commission has recommended the creation of a National Intelligence Director ("NID") with authority to manage the national intelligence program. The Commission has also recommended the NID have three deputies—for foreign intelligence, defense intelligence and homeland intelligence, respectively. The Commission has further recommended that the position of deputy NID for homeland intelligence be filled by either the FBI's executive assistant director for intelligence or the under secretary of homeland security for information analysis and homeland protection.

a. Why did the Commission leave the occupancy of this position somewhat indeterminate, as between the FBI and the Department of Homeland Security ("DHS")? Do you envision a rotating assignment of this authority? Are you concerned that you may be creating an unnecessary conflict between the FBI and DHS?

b. If the FBI creates a separate career track for intelligence agents, and the head of the FBI's intelligence program reports directly to the NID, won't these changes result in the *de facto* creation of a new domestic intelligence agency? If not, why not?

3. Most of the Commission's recommendations deal with changes in the federal government's approach to fighting terrorism, but your Report also recognizes the vital need to engage our state and local law enforcement officers more fully in the war on terror. The Report acknowledges the role of the FBI's Joint Terrorism Task Forces in this effort, and the importance of improved, reciprocal information sharing. Your report

also notes the critical role played by DHS in fostering communication with state and local officials. Can you share your perspective on the federal government's progress, or lack of progress, in more effectively sharing information with state and local authorities?

4. The 9/11 Commission Report suggests a two-pronged strategy that includes: (1) dismantling the Al Qaeda network and (2) prevailing over the ideology that gives rise to Islamic terrorism. With regard to the second prong, your report mentions the need to engage in the "Struggle of Ideas" to "encourage reform, freedom, democracy, and opportunity" throughout the Muslim world. Do you believe the democratic ideals espoused by the United States are compatible with the principles of Islam? Are there particular Islamic teachings, precepts or figures that can be held up as an alternative to the brand of fundamentalism advocated by Bin Laden and his cohorts?

5. Your Report recommends extensive measures to enhance border security and screening, such as the speedy implementation of a biometric entry-exit system, increased screening of passengers in order to detect explosives, and more integration and sharing of information with other countries. Your Report also notes, however, that these measures represent increased intrusions into the lives of our citizens. With respect to the protection of civil liberties, do you have particular concerns about the implementation of specific security measures? If so, which ones?

**QUESTIONS FROM SENATOR PATRICK LEAHY
FOR 9-11 COMMISSION VICE CHAIR LEE HAMILTON AND
COMMISSIONER SLADE GORTON**

1. The Commission Report recommends creating a National Intelligence Director who would "approve and submit nominations to the president of the individuals who would lead" each intelligence agency, including the FBI Intelligence office. The Commission also recommends creating three deputy positions under the NID, with the deputy for homeland intelligence possibly being the FBI's Executive Assistant Director for Intelligence. I would like a better understanding of how the Commission views the role of the FBI Director and the Attorney General in this new structure. You clarified at the hearing that, under the Commission's proposal, the FBI's Executive Assistant Director for Intelligence would continue to be accountable to the FBI Director and the Attorney General. But if the NID has budgetary control over the FBI's intelligence division and the hiring and firing authority over the Executive Assistant Director for Intelligence, what authority would the Attorney General and FBI Director have to ensure our domestic intelligence efforts are in compliance with the law?

2. The Commission Report identifies serious problems within the FBI with regard to both computer technology and the foreign language translation program. I was puzzled, therefore, to see that your recommendations to the FBI did not address these problems directly. Did you feel that Director Mueller has adequately addressed these issues? Did you consider but fail to reach consensus on recommendations in these areas? Or was there some other reason that these problems were not singled out for attention in the recommendations?

3. FBI oversight hearings I chaired in the 107th Congress brought to light several specific areas in need of reform. These include, first, the need to strengthen whistleblower protections for FBI employees in order to protect them from retaliation for reporting wrongdoing; and second, the need to improve the quality and constructive nature of the dialogue between the Bureau and Congress. Both issues are addressed in the FBI Reform bill (S.1440) that I introduced with Senator Grassley last year. Do you agree that these are critical areas in need of reform?

4. The Commission calls for enhanced congressional oversight of intelligence and homeland security. Senators Grassley and Specter and I have introduced legislation (S.436) designed to strengthen congressional oversight of foreign intelligence surveillance. Do you support greater public information on the use of FISA?

5. The Report paints a stark picture of the security status of the northern border before the 9/11 attacks. It details how Congress rejected attempts to increase security personnel at the border "despite examples of terrorists entering from Canada, awareness of terrorist activity in Canada and its more lenient immigration

laws, and an inspector general's report recommending that the Border Patrol develop a northern border strategy." I led the effort to increase personnel at the northern border, writing the provision in the USA PATRIOT ACT that tripled the number of Border Patrol agents, INS Inspectors, and Customs agents at our northern border. What other steps do you believe Congress should take to secure our border with Canada?

6. The Report states that "new insights into terrorist travel have not yet been integrated into the front lines of border security." What are the most important things Congress can do to assist in rectifying that weakness?

7. The Report makes a number of recommendations that involve working more closely with foreign governments in order to prevent unwanted travelers from reaching our shores. To what extent, then, is the protection of our borders an enterprise that requires international cooperation? Do you believe the United States can convince a substantial number of other nations to share their own "watch lists" with our consular and immigration officers?

8. The Report describes an INS that was "seriously hampered by outdated technology and insufficient human resources" a decade ago. How would you characterize the technology and resources of the immigration-related agencies in the Department of Homeland Security?

9. The Report states that the Attorney General gave no direction either to the FBI or the INS after receiving briefings during the summer of 2001 about terrorist threats, and as a result, "the borders were not hardened." What steps do you believe the Attorney General should have taken?

10. The Hart-Rudman Terrorism Task Force Report found that our nation will fall approximately $98.4 billion short of meeting critical emergency responder needs through this decade's end if current funding levels are maintained. Yet the Administration proposed a cut of $800 million to our police, fire and rescue squads in this year's budget by reducing overall first responder funding from $4.3 billion last year to only $3.5 billion this year. Would you agree that to be truly protected from, prepared for and able to respond to future terrorist attacks, we should dramatically increase funding to our nation's state and local first responders rather than decrease funding?

11. The Commission recommended the establishment of a civil liberties protection board within the executive branch to oversee adherence to the Commission's recommendations and to ensure our civil liberties are not sacrificed in the name of security. On August 27, 2004, President Bush signed an Executive Order (EO) creating the President's Board on Safeguarding Americans' Civil Liberties. The Board created in the EO will not have any non-governmental members and will not have independent investigative authority. The EO does not require that reports by the Board be made public. In addition, reports requested of Federal

agencies by the Board will not necessarily be accessible to the public. In short, the President's Board will have no authority, no independence from the executive branch, and no public accountability.

(A) What is the position of the 9-11 Commission on the President's Board as described in the EO? Specifically, do you believe that the Board should have the following characteristics:

1. Members from outside the government as well as agency representatives?
2. Independent investigative authority?
3. Regular reports to Congress and the public on the status of civil liberties in the United States?
4. Periodic reports to Congress and the public resulting from investigations undertaken by the Board?

(B) Would you support legislation to create a Civil Liberties Protection Board that includes all of the characteristics noted above in (a)?

12. You have recommended that the federal government set standards for identification documents, such as drivers licenses.

(A) What does the Commission contemplate by "standards?" For example, does "standards" mean particular issuance processes, protocols, technology interoperability and security features (e.g, biometrics, raised seals, holograms), or rather standardizing the type of information and format for the cards? Should biometric identifiers be one of the standards for identification documents, and if so, which biometric(s)?

(B) How should standards be developed, and what government agencies or entities should oversee that development?

(C) The Commission's report stopped short of recommending a national identification card, but acknowledged that standardization of identification documents may lead to a national identification card. Please detail the concerns prevented the Commission from endorsing a national identification card?

(D) Is there a benefit to relying on multiple, secure forms of identification, rather than a single identification document, which might limit opportunities for corroboration if compromised or authenticity is questioned?

(E) Has the Commission reviewed the work of the Document Security Alliance, a multi-agency collaboration that has produced a set of guidelines and best practices for the issuance of IDs?

Senate Judiciary Committee
Hearing on "The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security"
August 19, 2004

Written Questions Submitted by Senator Russell D. Feingold

Questions to Commissioners Lee Hamilton and Slade Gorton

1. The 9/11 Commission notes the need for the Transportation Security Administration (TSA) and the rest of the Department of Homeland Security (DHS) to have a comprehensive forward-looking strategic plan -- analyzing assets, risks, costs, benefits, etc. Three years after September 11th, we still, by and large, do not have such assessments to guide our spending. In the meantime, Congress and the President are spending billions of dollars on homeland security.

a. Based on your sense of what those homeland security priorities should be, do you believe Congress is dedicating sufficient funding for the most important homeland security priorities?

b. Could you comment on whether Congress is adequately funding first responders? Is Congress in the right ballpark, or, as a 2003 Council on Foreign Relations report found, are first responders "Drastically Underfunded, Dangerously Unprepared"?

2. The Commission report makes some important points about the need for, and ways to ensure, better congressional oversight of the executive branch. As former members of Congress, however, you both know well that Congress often faces resistance from the executive branch to such oversight. We regularly have problems getting executive branch officials to testify, for example, or even to answer our written questions in a timely manner. Are there ways to encourage the executive branch to be more responsive to congressional oversight, to treat Congress as a productive partner rather than a nuisance in our mutual efforts to combat terror?

3. The Commission recommends that homeland security funding be based on risk and vulnerability assessments. A conventional interpretation of this recommendation is that it would result in directing the vast majority of federal dollars to major cities such as New York and Washington, D.C. But how does the Commission recommend that Congress balance the desire to focus homeland security dollars on likely targets with the fact that in some scenarios, national infrastructure would be required to cope with an attack? For example, some bioterrorism attack scenarios involving infectious disease clearly require a strong

and efficient public health capacity nationwide. In addition, the report demonstrates that terrorists play close attention to security enhancements and vulnerabilities in this country. If we devote most of our spending to major cities, might not that encourage strikes against less well-defended locations or the use of such locations for planning and preparation?

4. Dr. Stephen Flynn warns in his new book: "If September 11, 2001, was a wake-up call, clearly America has fallen back asleep." The *New York Times* recently reported that almost half of midsize companies have not been spending any more money on security after September 11th than they did before that tragic day. There has also been a lot of discussion recently about the way in which the government should communicate warnings and risks to the general public. Everyone gets anxious for a few days or weeks and then it seems to be back to business as usual. Dr. Flynn also writes that "a democracy will not make hard decisions unless its citizens understand both the facts and the stakes involved." How should the federal government be communicating the facts and stakes involved? How should the federal government be mobilizing the nation - the public, the private sector, government - to adjust to the new realities that your report documents so well?

5. The Commission concluded that "compatible and adequate communications among public safety organizations at the local, state, and federal levels remains an important problem." Wisconsin public safety officials have told me the same thing, and they are working hard with the resources they have to address this serious shortcoming. But they are having a tough time, especially with the lack of sufficient federal funding and a clear federal plan. One part of your recommendation is to establish signal corps for high-risk urban areas that would ensure communications connectivity and to give this signal corps high funding priority.

a. Could you describe what the Commission had in mind operationally when it recommended establishment of these signal corps? What would a signal corps look like? Would it be like the recently announced RapidCom 9/30 program?

b. Is the Commission recommending this signal corps concept as a model for tackling the massive interoperability problem nationwide?

SUBMISSIONS FOR THE RECORD

WASHINGTON LEGISLATIVE OFFICE
Laura W. Murphy
Director

915 15th Street, NW Washington, D.C. 20005
(202) 544-1681 Fax (202) 546-0738

American Civil Liberties Union

Statement for the Record
at a hearing on
"The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security"

before the
Senate Judiciary Committee

Submitted by

Gregory T. Nojeim,
Associate Director and Chief Legislative Counsel

and Timothy H. Edgar
Legislative Counsel

August 19, 2004

American Civil Liberties Union
Statement for the Record at a hearing on
"The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security"
before the Senate Judiciary Committee
Submitted by Gregory T. Nojeim, Associate Director and Chief Legislative Counsel and Timothy H. Edgar, Legislative Counsel

August 19, 2004

Chairman Hatch, Ranking Member Leahy and Members of the Committee:

We are pleased to submit this statement for the record on behalf of the American Civil Liberties Union and its more than 400,000 members, dedicated to preserving the principles of the Constitution and Bill of Rights, to explain the ACLU's views on the recommendations in the Final Report of the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission report").

The 9/11 Commission report exhaustively details significant failures of the intelligence agencies, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA), and proposes major structural changes to address those failures. The report contains helpful suggestions on privacy and civil liberties, proposing a Civil Liberties Protection Board and a framework for judging anti-terrorism powers including the USA PATRIOT Act. The report also endorses more effective oversight of the intelligence community, and real reform of excessive secrecy.

The report also contains detailed discussion of border and transportation security issues, including airline screening, the "no fly" list that has stranded many innocent travelers, and passenger profiling. By endorsing an expansion of intrusive border screening to domestic travel, the report's recommendations could – if implemented without change – result in a "checkpoint society" in which a federally-standardized drivers license serves as a "national ID" and internal passport.

As the 9/11 Commission itself acknowledges, "many of our recommendations call for the government to increase its presence in our lives . . . ." (p. 395). In fact, as outlined, a number of specific proposals could have serious unintended consequences that would be highly detrimental for basic civil liberties. Legislation must include significant changes to some recommendations to protect civil liberties. The Commission's proposals to advance civil liberties – including increased oversight, reduced secrecy and a Civil Liberties Protection Board – must be implemented to ensure that, as the government centralizes some powers, it provides stronger checks and balances.

No one doubts the necessity of reorienting an intelligence community built to fight the Cold War to focus on the national security threats of the 21st Century. The ACLU strongly favors reforming the intelligence community in a way that enhances national security, encourages openness, and protects civil liberties.

This testimony outlines specific recommendations for how to implement the reforms proposed by the Commission without eroding basic freedoms.

The National Intelligence Director and National Counter-Terrorism Center

Recommendation #1: The National Intelligence Director (NID) should not be a Cabinet or White House official and the National Counter-Terrorism Center (NCTC) should not placed in the Executive Office of the President, nor should stronger community-wide powers be given to an official who continues to head the CIA. A new head of the intelligence community, if one is created, should instead head an independent Office of the Director of National Intelligence.

In a democratic society, domestic surveillance must serve the goals of preventing terrorism, espionage and other serious crime, not the political goals of the party in power. As we have learned from past mistakes, the temptation to use the intelligence community to further a political agenda is ever-present.

Misuse of both foreign and domestic intelligence powers for political ends can occur under any Administration. Direct White House control of intelligence powers and access to sensitive intelligence files have been responsible for serious mistakes that undermine civil liberties and accountability, and have lessened the confidence of Americans in their government. For example, the worst spying abuses of the Nixon Administration were directed by White House staff with intelligence backgrounds and included warrentless secret searches to obtain medical records, covert wiretaps of journalists, and the Watergate break-in itself. Under President Reagan, a covert operation conducted by National Security Council staff member Lt. Col. Oliver North led to the most serious crisis of Reagan's presidency when it was revealed that the operation involved trading arms for hostages and using the proceeds to provide assistance to Nicaraguan rebels. Under President Clinton, White House political staff obtained hundreds of confidential FBI files on prominent Republicans that had been created from extensive background checks designed to protect national security.

In spite of these lessons, the 9/11 Commission's recommendations place effective control over the intelligence community – including parts of the FBI, Department of Homeland Security, and other agencies that exercise domestic surveillance powers – in the Executive Office of the President (the White House) and fail to include any mechanism (such as a fixed term) to ensure the National Intelligence Director's autonomy. The proposal seriously increases the risk of spying for political ends.

The proposed structure centralizes too much power over both foreign and domestic intelligence in the White House, and risks a re-run of the mistakes that led to Watergate, Iran-*contra*, "Filegate," and other significant abuses of Presidential power.

The placement of the National Intelligence Director in the White House could also frustrate Congressional oversight. White House officials have long received, on

separation of powers grounds, far less scrutiny from Congress than agency heads and other Executive Branch officials. White House officials are not usually subject to Senate confirmation and do not usually testify before Congress on matters of policy. Executive privilege may be claimed as a shield for conversations between the President and his advisors from both Congressional and judicial inquiries.

President Bush announced on Monday, August 2, a proposal for a national intelligence director that is not a White House or Cabinet official, but instead heads an independent office. Likewise, bills proposed by leading Democratic members of the House and Senate intelligence committees do not make that person a White House official.

Rep. Jane Harman, the ranking member of the House Permanent Select Committee on Intelligence, has introduced legislation to create a "Director of National Intelligence." Like President Bush's proposal, H.R. 4140, the "Intelligence Transformation Act," places the new intelligence director in an independent office, not the White House. The leading Senate legislation takes the same approach. Senate bills include S. 190, the "Intelligence Community Leadership Act of 2003," sponsored by Senator Feinstein (D-CA) and S. 1520, the "9-11 Memorial Intelligence Reform Act," sponsored by Senators Graham (D-FL), Feinstein (D-CA) and Rockefeller (D-WV).

The ACLU supports placing a new intelligence director in an independent office. The National Intelligence Director and the National Counter-Terrorism Center, if they are established, should be accountable to the President, but they should not be servants of the President's political or ideological agenda.

Pitfalls of greater power for head of the CIA. Rep. Porter Goss (R-FL), President Bush's nominee for Director of Central Intelligence (DCI), has introduced a different intelligence reorganization bill, H.R. 4584, the "Directing Community Integration Act." The Goss bill rejects a new intelligence director and instead enhances the powers of the DCI over community-wide responsibilities, including domestic collection of intelligence, while leaving the DCI as the head of the CIA.

The Goss bill is, in some respects, even worse than the Commission's proposal for a White House NID, because it contemplates much greater involvement of the DCI – the head of a foreign intelligence agency – in domestic intelligence matters. The Goss bill would even go so far as to render toothless the current prohibition on CIA involvement in domestic activities by amending it to bar "police, subpoena, or law enforcement powers within the United States, *except as otherwise permitted by law or as directed by the President.*"[1]

The proposed amendment would erase a fundamental limitation on CIA authority that prevents the use of CIA-style covert operations and intelligence techniques – including warrantless surveillance, break-ins, and infiltration and manipulation of political groups – from being used in the United States against Americans.

[1] H.R. 4584 § 102(a) (amending 50 U.S.C. § 401-1(c) and repealing § 403-3(d) (emphasis added)).

Recommendation #2: The National Intelligence Director must be subject to Senate confirmation and Congressional oversight, and should, like the Director of the CIA, have a fixed term that does not coincide with that of the President.

Congress must ensure that the National Intelligence Director is appointed by and with the advise and consent of the Senate, and that the NID will regularly testify before Congress. The Office of the NID and the NCTC must also be answerable to Congress. Congress must make clear that key officials will be asked to testify and that the NID and the NCTC are expected to provide answers to questions, relevant documents, and cooperate with Congressional inquiries.

The Commission recommends that the Director of the CIA should serve a fixed term, like the Director of the FBI, that does not coincide with the President's term. Insulating the CIA further from political pressure is a welcome step.

Ensuring the intelligence community works well together is an extremely important responsibility that must remain above partisan politics or the appearance of serving an ideological agenda. The President should, of course, appoint the National Intelligence Director, with Senate approval, and should retain the power to fire the director for poor performance. As with the head of the FBI or the Chairman of the Federal Reserve Board, however, the director should serve a fixed term that does not coincide with the President's term.

Recommendation #3: To ensure the FBI retains control of domestic surveillance operations, the head of the FBI's intelligence operations must report to the FBI Director and the Attorney General, not to the National Intelligence Director or another intelligence official.

The United States has – historically and to the present day – entrusted the domestic collection of information about spies, terrorists, and other national security threats to federal and state law enforcement, with the FBI playing the most important role. The reason is simple: Americans do not believe the government should investigate you if you are not involved in a crime – if your activities, however unpopular, are not illegal.

For this reason, the CIA – a pure spy agency with no law enforcement functions – has been barred from domestic surveillance ever since it was created by the National Security Act in 1947. President Truman – a strong opponent of Communism and a hawk on security – shared the concerns of many Americans about the CIA's establishment as a peacetime agency. Truman believed that a permanent secret spy agency could, if allowed to operate on American soil, use espionage techniques – including blackmail, extortion and disinformation – against American citizens who were critical of government policy or the incumbent administration, but had broken no law. With Truman's support, the National Security Act, sometimes described as the CIA's "charter," contains a prohibition – which stands today – on the CIA's exercising any "police, subpoena, or law enforcement powers or internal security functions."[2]

[2] 50 U.S.C. § 403-3(d)(1).

Truman's concerns were not just with bureaucratic turf – whether the FBI or the CIA was the lead agency in collecting information about national security threats within the United States. Truman believed that the domestic collection of information about national security threats should generally be handled as a law enforcement matter. Indeed, Truman often clashed with FBI Director Hoover over whether the FBI had any business using break-ins, illegal wiretaps, and other spy techniques, at one point saying Hoover's advocacy of such methods risked transforming the FBI into the equivalent of the Gestapo.[3] Truman did not just want to prevent the CIA itself from operating on American soil – he wanted to ensure that a CIA-style agency did not become dominant in domestic collection of intelligence about national security threats.

The 9/11 Commission proposes that the NID hires both the FBI's Director of Intelligence and the intelligence chief of the Department of Homeland Security, either of whom may serve as the deputy NID for homeland intelligence. This proposal is very problematic. The Commission proposal puts the FBI's intelligence capabilities in the hands of a super-spy who could involve in domestic spying officials of the CIA and other agencies that use the methods of agencies that operate overseas – such as break-ins, warrantless surveillance, or covert operations.

While a NID could play a role in coordinating the activities of the Intelligence Community, the NID should not be given, as the Commission's proposal currently contemplates, what amounts to control over targets of intelligence collection within the United States. That should remain the responsibility of the FBI Director, under the supervision of the Attorney General.

Recommendation #4: The FBI Director and the Attorney General should have the responsibility to ensure that the guidelines and rules that govern domestic surveillance in both criminal and national security investigations are followed. The guidelines must be strengthened. While they may continue to allow "enterprise investigations" of criminal organizations including foreign and domestic terrorist organizations, they should clearly prohibit domestic spying on First Amendment-protected activity.

The FBI's own mistakes and missteps show the dangers of a powerful government agency that uses its investigating authority without regard to whether the subjects of its investigations are involved in criminal activities. To a large degree, these abuses were the result of the FBI's unique lack of accountability to the courts, Congress and even the Attorney General under the direction of FBI Director J. Edgar Hoover.

Today, as a result of the Church Committee reforms, the FBI operates under both internal and external controls that constrain its criminal and national security investigations. These controls are designed to ensure that its intrusive intelligence-gathering and criminal surveillance powers are directed at organizations involved in criminal activities and at the investigation of foreign agents and not at lawful political, religious and other

[3] *See* Curt Gentry, *J. Edgar Hoover: The Man and the Secrets* (2001).

First Amendment activities. Controls that protect civil liberties include guidelines for FBI investigations, constitutional limits enforced by the exclusionary rule, and the "case-oriented" focus of the FBI. Putting a spy chief in charge of parts of the FBI could seriously erode each of these controls.

Domestic terrorism guidelines. For criminal investigations of organized crime or domestic terrorism, Attorney General guidelines restrict the use of most surveillance techniques – such as tracking mail, following suspects, and interviewing witnesses – to situations where there is at least some indication of criminal activity. These guidelines were weakened, following September 11, to allow FBI agents to visit, on a clandestine basis, political and religious meetings that are "open to the public" without any such indication. The ACLU and many members of the House and Senate judiciary committees opposed this change. Most other investigative techniques still do require at least some indication of crime.

International Terrorism Guidelines. National security investigations of international terrorist groups are governed by separate guidelines, important parts of which are secret. The guidelines do not require probable cause of crime but are, in theory, designed to restrict national security investigations to circumstances in which there is some indication of hostile activity by an agent of a foreign power. The most intrusive national security investigations – those that involve physical searches or electronic eavesdropping – must also at least "involve" some possible criminal activity when the subject of the investigation is a United States citizen or permanent resident, although this falls far short of the constitutional standard of criminal probable cause.

Investigative guidelines are vitally important to preserving civil liberties. The government argues that a number of highly intrusive intelligence gathering techniques – including collecting files on individuals and groups, physical surveillance in public places, and tracking the sender and recipient of mail, telephone and Internet communications – are not constitutional "searches" subject to the Fourth Amendment's probable cause standards. As a result, for investigations using such techniques, it is only the guidelines and case-oriented structure of the investigating agency that protects against widespread spying on lawful political and religious activities.

The Constitution and the exclusionary rule. For those intrusive techniques that the government concedes are searches – including electronic eavesdropping of the content of communications and searches of a person's home or office – the Fourth Amendment and federal statutes plainly require court approval based on probable cause. However, the Fourth Amendment's principal remedy, the exclusionary rule that provides illegally-obtained evidence may not be used in court, does nothing to hinder illegal searches and wiretaps if the government does not plan to use the information in a prosecution.

The danger is certainly exacerbated by putting the FBI's intelligence operations in the hands of the government's "top spy" instead of its "top cop." The FBI Director could, of course, direct abuses on the theory that the information is to be used for intelligence purposes rather than criminal prosecution and so need not be gathered legally. The

danger would be far greater, however, if the FBI's national security operations are under the effective control of intelligence officials who are used to operating entirely outside the constraints of the exclusionary rule.

The FBI's case-oriented approach. The FBI's focus on both criminal and intelligence "cases" helps prevent highly intrusive and sensitive investigations that may involve religious and political activities that are protected by the First Amendment from losing all focus on crime and terrorism. This focus is vitally important to civil liberties, and could be lost if a spy chief is placed in charge of parts of the FBI.

Critics of placing the FBI in charge of domestic national security surveillance argue that the case-oriented mindset of a law enforcement agency cannot be reconciled with quality intelligence analysis. While the FBI concerns itself with gathering information of relevance to particular cases, they argue, intelligence analysts must be looking more broadly to see how specific data fits into the "big picture" of a national security threat.

This critique sweeps too broadly because it fails to recognize the difference between two very different kinds of cases. The FBI not only investigates particular crimes – generally, crimes that have already occurred and must be "solved" – it also opens "enterprise" investigations of organized crime and terrorism. For example, in investigating a domestic funding network for Al Qaeda as a possible criminal enterprise, the FBI is not limited to investigating whether the organization was involved in funding specific terrorist bombings or other attacks, such as the 1998 embassy bombings in Africa, the 1999 bombing of the U.S.S. Cole, or the September 11 attacks. Rather, the FBI has authority to investigate the organization as an enterprise, and to fit together bits of information that help prevent future terrorist attacks, not just gather information about past crimes. The FBI's failures in analyzing information about Al Qaeda's domestic activities are not a result of flaws in the basic concept of an enterprise investigation; rather, they appear to be the result of a combination of other failures that must be addressed on their own terms.

Recommendation #5: The powers of the NID and the National Counter-Terrorism Center should be specified by a statutory charter that prohibits powers not authorized and requires the NID to observe guidelines to protect against domestic spying on First Amendment activity. Explicit, enforceable statutory language should make clear that the NID does not have what amounts to operational control of targets of domestic surveillance, whether directly or through the NCTC.

The Commission proposes a powerful new National Counter-Terrorism Center under the authority of the NID. The Center, while not itself a domestic collection agency, would go beyond the analysis of intelligence collected in the United States and abroad that is the function of the existing Terrorism Threat Integration Center (TTIC). If the Center's powers are not specified, and if it is not barred from monitoring First Amendment activities within the United States, the Center could task domestic collection efforts that seriously erode the limits the collection agencies themselves are bound to respect.

The Center would be structured like the CIA. The Center would have separate divisions for "intelligence" and "operations." It would have the authority to "task collection requirements" and to "assign operational responsibilities" for all intelligence agencies – including the FBI – and to follow-up to ensure its mandates are implemented.

The Center's power over both intelligence collection and operations throughout the intelligence community could pose grave risks of encouraging espionage and covert operations techniques on American soil. The Center's tasking and strategic planning functions would extend not only to the FBI's national security investigations, but also to other domestic agencies, including the Department of Homeland Security, with immigration, border control and transportation security functions.

Likewise, some of the powers of the NID and the Center over the intelligence agencies of the Department of Defense – the largest agencies, consuming the large majority of the intelligence community's budget – could have domestic implications. The Department of Defense, after September 11, established a powerful regional Northern Command (NORTHCOM), led by a four-star general, with responsibility for the domestic United States (together with Mexico and Canada).

NORTHCOM already has a military intelligence unit, which raises serious questions under the Posse Comitatus Act – the law that limits military involvement in domestic affairs. Under the proposed structure, the NID and the Center could have what amounts to control of the domestic intelligence operations of civilian federal law enforcement and of the NORTHCOM intelligence unit, creating a real risk of blurring the military and civilian functions.

Recommendation #6: The National Intelligence Director and the National Counter-Terrorism Center should not be permitted to direct or plan intelligence "operations" that include "dirty tricks" or other extra-legal methods within the United States. Domestic use of intelligence information must remain bound by the legal system.

Perhaps the most far reaching power of the National Counter-Terrorism Center is its authority to plan and direct intelligence "operations" throughout the intelligence community. If the NID and the NCTC are created, it must be made clear that information derived from domestic surveillance is only to be used within the bounds of the legal system, and cannot be used for domestic "operations" outside that system.

The FBI's COINTELPRO operations – "counterintelligence" programs under FBI Director J. Edgar Hoover that both gathered intelligence and used that intelligence to disrupt perceived national security threats – led to extremely serious abuses of power. These abuses included the illegal wiretapping of Martin Luther King, Jr. and the infiltration of scores of social, political and religious groups that opposed government policy, as well as "dirty tricks" campaigns to exploit damaging information without exposing the FBI's sources and methods in a criminal prosecution.

The COINTELPRO programs were initially rationalized as attempts to counter what Hoover perceived as the influence, or possible influence, of the Soviet Union on the civil rights and anti-war movements. However, a lack of internal or external controls led to the continuation of these highly intrusive operations without any real evidence of involvement of a genuine agent of a foreign government or organization and without an indication of criminal activity. In other words, the FBI's most serious abuses of civil liberties occurred precisely when its top leadership forgot it was a law enforcement agency operating to enforce and uphold the law – not a freestanding security or spy agency designed to counter those individuals and groups whose views seemed, to the government officials, to be dangerous or un-American.

If the powers of the National Counter-Terrorism Center are not properly limited, the result could be the establishment of what amounts to just such a freestanding spy agency in all but name. For civil liberties reasons, the 9/11 Commission soundly rejected the idea of moving the FBI's counter-intelligence and intelligence gathering functions to a separate agency patterned on the UK's Security Service or MI-5. The FBI, because of its mission and culture, can serve the intelligence gathering mission that the CIA serves overseas, but the FBI must operate under the U.S. Constitution and "quite different laws and rules." The Commission was also sensitive to the dangers of negative public reaction to civil liberties abuses that would result from creating an agency unconstrained by those rules. A "backlash," it says, could "impair the collection of needed intelligence."

It also objects to the MI-5 idea for these reasons:

- The creation of a new agency, and the appearance of another big kid on the intelligence block, would distract the officials most involved in counter-terrorism at a time when the threat of attack remains high.

- The new agency would need to acquire, train and deploy a vast amount of new assets and personnel, which the FBI already has at its disposal.

- Counter-terrorism very easily ropes in matters involving criminal investigation. With the removal of the pre-9/11 "wall," it makes logical sense, the commission says, to have one agency utilize the entire range of intelligence and criminal investigative tools against terrorist targets.

- In the field, the cooperation between counter-terrorism investigators and the criminal side of the FBI has many benefits.

The Commission was right to reject the model of a domestic intelligence agency. For much the same reason, however, its proposals for intelligence reform must be modified and clarified.

Reducing Excessive Secrecy and Strengthening Oversight of the Intelligence Community

As the 9/11 Commission observes, structural reform of the intelligence community will not by itself solve basic intelligence deficiencies that contributed to recent intelligence failures. Substantive reforms – including strong internal watchdogs and a civil liberties board, a reduction in excessive secrecy, an increase in real public and Congressional oversight, and stronger efforts to incorporate dissenting views into analysis – must be adopted to prevent future intelligence breakdowns.

Recommendation # 7: The Commission recognized its recommendations could increase government intrusion on civil liberties and urged strong oversight. Congress should not act to reorganize the intelligence community without also implementing the Commission's proposals for strong internal watchdogs and an effective civil liberties protection board.

Strong internal watchdogs. Proposals to reform the intelligence community have included the creation of an Inspector General for the intelligence community. The Inspector General would have significant investigative powers, including subpoena power, that would aid internal investigations. An Inspector General for the intelligence community would report directly to the National Intelligence Director and, as a result, could be a more powerful, and more independent, watchdog than the inspectors general that currently have jurisdiction over each of the fifteen intelligence agencies.

Civil liberties protection board. The 9/11 Commission should be commended for recognizing the need to protect civil liberties and endorsing an independent watchdog board to strengthen oversight throughout the government. While various entities and offices within the Executive Branch, such as inspectors general, officers for civil rights and privacy, and oversight boards, are charged with policing certain departments, agencies or programs, no one board has the responsibility for ensuring that civil liberties are not compromised by the need for enhanced security.

The need for such an independent, nonpartisan voice is clear. The Commission recommends putting the burden of proof on the government to show the need for new security powers, such as those enacted by the USA PATRIOT Act, but there is no reliable, independent agency that performs this function. The Commission did not, however, set forth any specific proposals with respect to what a civil liberties board could do.

The 9/11 Commission observed:

> "[D]uring the course of our inquiry, we were told that there is no office within the government whose job it is to look across the government at the actions we are taking to protect ourselves to ensure that liberty concerns are appropriately considered. If, as we recommend, there is substantial change in the way we collect

and share intelligence, there should be a voice within the executive branch for those concerns."

The Commission proposes a board that would "oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties."

The recommendation implicitly recognizes that that there is a need for two functions, one proactive and one retrospective. First, a board should be a proactive voice for civil liberties during the development of counter-terrorism policies. For example, during the development of the government's "no fly" list, the board should be asked to study and address civil liberties concerns. How are persons who are mistakenly put on such a list to get off the list? How will the government ensure that innocent travelers who have the same or similar name to a person on the "no fly" list are not harassed?

Second, a board must be able to look retrospectively at patterns of civil liberties abuse, or at significant new programs or laws that intrude on civil liberties. The board could, for example, examine the treatment of terrorism suspects detained on immigration violations or as "material witnesses," but not charged with terrorism. The board could also look at the effectiveness, and impact on civil liberties, of new powers, such as the USA PATRIOT Act, and issue a report prior to the expiration of such powers.

This investigative function should build on the work of others, including the inspectors general of the agencies involved. Because those offices do not have government-wide authority, a board must be able to have the discretion to review and assess the work of inspectors general and other existing investigators, and to go further where necessary.

To complete its objectives, the board must have substantial clout, authority, and powers. It should be bipartisan. Ideally, appointments should be shared between the President and Congressional leaders, if such an appointment process can be reconciled with separation-of-powers concerns. Board members should have independence and should serve a fixed term, and they should be prominent citizens with experience in civil liberties, government investigations, and security. The board should hire an full-time executive director and a staff that permits it to carry out its functions.

The board should have the power to hold public hearings and issue both annual reports assessing the state of civil liberties and special reports that detail the results of investigations. Agencies should be required to respond to their recommendations, and the board should also make recommendations, where appropriate, for legislation. The board should have the power to subpoena documents and witnesses, and should enjoy the cooperation of all departments. Members and staff should have high-level security clearances to enable the examination of even the most sensitive national security secrets.

Recommendation #8: A presumption against classification without good reason was contained in Executive Order 12958 but has been rescinded. As a first step in reforming an outmoded system of secrecy designed for the Cold War, the presumption should be reinstated.

As the 9/11 Commission report recognized, excessive classification – not civil liberties protections – almost certainly represents the greatest barrier to effective information sharing. As the report states, too often the attitude has been that "[n]o one has to pay the long-term costs of over-classifying information, though these costs . . . are substantial." The report laments an outdated, Cold War-era "need to know" paradigm that presumes it is possible to know, in advance, who requires access to critical information. Instead, it recommends a "'need-to-share' culture of integration."

"Groupthink" led to some in the government discounting the possibility that Al Qaeda terrorism was directed at the United States, rather than overseas. According to the Senate Select Committee on Intelligence, groupthink was also the major culprit behind the intelligence failures regarding Iraq's WMD programs. Groupthink cannot be challenged in secret. Public pressure – including the media and public interest groups – can challenge government agencies to reassess their assumptions.

Unfortunately, the Bush Administration has moved in the opposite direction – towards greater secrecy. President Bush's executive order on classification, issued after September 11, not only extended a deadline for automatic declassification of old documents, it actually reversed a presumption against classification without good reason that was put into place by President Clinton in 1995 as a signal to agencies that their classification decisions should have stronger justification.[4]

Recommendation #9: The Freedom of Information Act should be amended to require courts to balance the public's need to have access to information that is critical for oversight of government – such as serious security flaws, or civil liberties abuses such as the mistreatment of detainees – against government claims that the information is exempt from disclosure.

"Need-to-share" cannot be limited to agencies within the government or defense and homeland security contractors, but also must include, to the greatest extent possible, sharing relevant information with the public. Congress and the Administration have created, through the Homeland Security Act, an entirely new category of information that is withheld from public view – sensitive but unclassified (SBU) information. While the 9/11 Commission criticizes excessive secrecy, it also endorses establishing a "trusted information network" for sharing of unclassified, but still nonpublic, homeland security information.

The Commission's calls for greater openness and sharing of information will not be effective if it succeeds only in adding another set of complex secrecy rules designed to limit public access to "homeland security information" on top of the existing classification regime. New categories of secret information – including "sensitive but unclassified," homeland security information, or information in a new "trusted information network" – may succeed only in replacing one unwieldy secrecy regime with

[4] Further Amendment to E.O. 12958 (March 25, 2003); *See* Adam Clymer, *U.S. Ready to Rescind Clinton Order on Government Secrets*, N.Y. Times, March 21, 2003.

another. The need for government and industry to keep critical infrastructure information from the public must be balanced against the public interest in access to critical oversight information. The Freedom of Information Act should be amended to require this.

Recommendation #10: Congress should enact S. 436, the Domestic Surveillance Oversight Act, or its House counterpart, H.R. 2429, the Surveillance Oversight and Disclosure Act, as a first step towards making more information about the use of FISA available to the public.

The Commission calls for a debate on the USA PATRIOT Act, putting the burden on the government to show why a given power is needed. However, the government still takes the position that its use of surveillance authorities under the Foreign Intelligence Surveillance Act (FISA) is classified, and that the public's right to know only extends to the total number of surveillance applications made and the total number of orders granted. There can be no meaningful debate on the government's use of the USA PATRIOT Act, which expanded FISA surveillance powers, without any publicly-available objective data on such basic matters as how many surveillance orders are directed at United States persons, how many orders are for electronic surveillance, how many are for secret searches of personal records, and so on.

Rep. Hoeffel has introduced legislation (H.R. 2429) that would provide more public information about the use of FISA, and Senators Leahy, Specter and Grassley have introduced a similar measure (S.436).

Recommendation #11: Congress should enact S. 2672, the Lott-Wyden bill, which establishes a bipartisan classification review board, or its House counterpart, H.R. 4855. Congress should consider enhancing the board's power to release improperly classified documents. The Senate Select Committee on Intelligence should also make clear it will wield its existing power under the Senate rules as an effective check against intransigence by the President in releasing classified information that the board recommends to be released.

The Congress should enact S. 2672, sponsored by Senators Trent Lott (R-MS) and Ron Wyden (D-WA), the "Independent National Security Classification Board Act of 2004." An identical bill, H.R. 4855, has been introduced in the House by Rep. Bud Cramer.

The bill would create a bipartisan board, appointed by the President and members of Congress, to review and reform classification rules. The board should consider whether a complex system of government secrets that has grown to include layers upon layers of bureaucratic rules is the best way to safeguard the national security, and recommend real reforms.

Recommendation #12: The intelligence committees should hold far more open hearings. The annual hearings on legislation authorizing the intelligence community – as well as other legislative hearings – should be open to the public.

The 9/11 Commission called for Congressional oversight to be greatly improved, calling the current structure "dysfunctional." As the Commission made clear, the establishment of a Senate and House committee devoted to intelligence matters does not provide effective oversight when hearings – even hearings on legislative matters – are almost always closed to the public

Recommendation #13: The intelligence budget should be made public as the Commission recommends.

Perhaps the most inexplicable example of excessive secrecy that frustrates real accountability is the continued insistence by the intelligence community on keeping basic information – even information that is widely known or guessed – classified. Even the overall amount of money budgeted for intelligence activities, which is widely reported as being approximately $40 billion, is classified as is the amount of money budgeted for components of the intelligence community. At least these numbers, and other information that would help the public know how its dollars are being spent, should be made available.

Recommendation #14: While Congress should consider ways to consolidate and strengthen oversight of the intelligence community, the intelligence community should not be shielded from the oversight of relevant committees. Most importantly, the House and Senate judiciary committees must retain jurisdiction that is concurrent with the intelligence and homeland security committees over domestic surveillance, access to the courts and other government actions that affect legal and constitutional rights.

The Commission's other recommendations include investing the intelligence committees, or a joint committee of both Houses of Congress, with authorizing and appropriations powers over the intelligence communities. This proposal should be approached with caution. Limiting the number of committees with jurisdiction over the intelligence community may frustrate oversight instead of enhancing it. If the single committee with jurisdiction over intelligence does not ask probing questions concerning a given program or policy, there will no longer be the potential for another committee to fill the void.

Most importantly, the judiciary committees of the House and Senate must retain concurrent jurisdiction over intelligence matters affecting legal and constitutional rights. A more powerful intelligence committee should *not* have the exclusive or final say on amendments to the Foreign Intelligence Surveillance Act or other sensitive surveillance statutes, for example. The same need for some concurrent jurisdiction in the judiciary committees arises if Congress adopts the Commission's proposal for permanent committees to oversee the Department of Homeland Security.

Recommendation #15: Congress should enact S. 2628, the Akaka-Grassley bill, or its House counterpart, H.R. 3281, the Platts bill, providing special protections for national security whistleblowers.

Finally, a thorough and comprehensive review of the treatment of national security whistleblowers must be part of any reform of the intelligence community. The role of whistleblowers in assisting our understanding of pre 9/11 intelligence failures has been essential.

National security whistleblowers face unique obstacles. Many intelligence and national security jobs are exempt from the civil service protections, including whistleblower protections, enjoyed by most government employees. National security whistleblowers also face additional hurdles, such as the loss of a security clearance or possible criminal charges for allegedly disclosing classified information, that are not faced by most government whistleblowers.

The 9/11 Commission's calls for reform of the intelligence community that would challenge conventional wisdom should include specific procedures that would encourage whistleblowers. Additional safeguards, consistent with national security, must be enacted to encourage employees who see distorted and sloppy analysis or other serious shortcomings to come forward without fear of losing their jobs, security clearances, or going to prison.

The USA Patriot Act

Recommendation #16: Congress should adopt the 9/11 Commission's framework for determining whether to extend controversial provisions of the USA PATRIOT Act when they expire next year, which puts the burden on the government to show why powers are needed *before* examining the impact on civil liberties. In particular, Congress should wait until next year to decide whether to re-authorize the sections of the law that sunset so as to preserve an adequate opportunity for the debate for which the Commission called.

During the rush to enact the USA PATRIOT Act after September 11, the White House and Attorney General implied that if changes to the law did not pass quickly, and there was another terrorist attack, the blame would rest on Congress. Not surprisingly, the law passed by wide margins: 96 to 1 in the Senate, 357 to 66 in the House. Since then, however, numerous lawmakers have expressed reservations, and many, including members of the Subcommittee, are actively seeking to refine the law to better protect civil liberties.

Congress wisely included a series of "sunset" provisions in the law, which would require Congress to reauthorize certain provisions or let them expire by December 31, 2005. The Administration has asked Congress to act this year to remove the sunset provisions, which would make the entire law permanent.

The 9/11 Commission report unequivocally said that the government has the responsibility for defending the expansions of government power that are the hallmark of the USA PATRIOT Act. The Commission could have, but did not, endorse the PATRIOT Act and call for its renewal. Instead, the Commission called for a "full and

fair debate" over the need for these new powers, with the burden of proof resting on the government to show why a power is needed. In our view, the Department of Justice has not to date met this burden – particularly with respect to the most controversial parts of the USA PATRIOT Act. These sections relate to secret searches and access to library and other records, either under a minimal level of judicial review under Section 215, or with no review at all in the case of National Security Letters in Section 505.

The 9/11 Commission also recommended that expansions of government power must come only with adequate supervision of the executive's use of the powers to ensure protection of civil liberties. This is a very important recommendation. We believe that enacting the Security and Freedom Ensured Act ("SAFE" Act), H.R. 3352 (and S. 1709 in the Senate) is an important step that Congress could take to increase judicial, Congressional and public supervision.

A National ID Card

Recommendation #17: Congress should reject any proposal to (1) make state-issued driver's licenses into a common license that is federally-designed, but issued by the states, (2) require licenses to contain an embedded computer chip bearing the holder's biometric identification information (i.e. a fingerprint or retina scan and digital picture), or (3) link the ability to obtain a drivers license to immigration status.

While the 9/11 Commission did not endorse a national identification card *per se*, its recommendations for federal standards for drivers licenses would almost certainly amount to a back-door way of accomplishing the same objective. Rep. Cannon (R-Utah) pointed this out at a hearing on August 20.

Even during periods of national threat, most notably the Cold War and World War II, the country has never thought it necessary to require citizens to carry "papers" with them at all times. If Congress did so now, it would endanger both security and civil liberties.

Once federalized, drivers licenses would be demanded for all manner of personal transactions that do not now require one. Moreover, federalized licenses would be the key that accesses personal information about the holder that would be inevitably linked to the license. Today, that information would include obvious identifiers such as Social Security Number and address. But tomorrow, it would include less obvious identifiers, and not just fingerprints and retina scans. Many businesses – from landlords to retailers – would themselves, or through the government, seek to tie personal information to the federalized drivers license, and they would not allow routine transactions unless a person produced their federalized drivers license.

Some states have decided that drivers licenses should be issued to those who can prove that they can drive, as opposed to those who can also prove that they are in the country lawfully. They have decided that it serves their public safety needs to ensure that all

drivers are licensed regardless of immigration status. Congress should not step in to upset this determination.

Moreover, the same people who produce fraudulent state identification documents today would produce fraudulent federalized identification documents tomorrow. The fraudulent federalized documents would be used not only by those seeking to commit fraud, but by those intending to do much more serious harm.

Finally, Congress has considered, and ultimately rejected, this proposal before. This proposal is very similar to Section 656(b) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. The regulation the Department of Transportation proposed to implement Section 656(b) was roundly criticized as a system of national identification, and was never implemented. The regulation that the DOT proposed drew literally thousands of negative comments from members of the public. Congress wisely repealed the provision in a subsequent transportation appropriations bill.

A much better approach would be for Congress to fund state efforts to make drivers licenses more secure.

Airline Passenger Profiling and "No Fly" Lists

Recommendation #18: Before the TSA begins administering no-fly lists, Congress should ensure that there is some independent review, subject to appropriate security measures, of how someone gets on the no-fly list. For travelers who find themselves wrongfully included in the no-fly list, there must be some process for them to clear their names, and the TSA should be required to track the number and cost (both to effectiveness and civil liberties) of "false positives."

The 9/11 Commission took no position on whether the passenger profiling system known as CAPPS II should go forward. Moreover, its factual findings suggest that the approach taken by the proposed CAPPS II – to subject every commercial air passenger to an invasive background check against business and intelligence databases -- is not necessary to ensure airport security.

However, the Commission did endorse broad expansions of "no-fly" and "automatic selectee" lists, and that screening against these lists should be performed by the Transportation Security Administration, instead of by the airlines, as is now the case.

The ACLU has long-standing concerns about the use of federal watchlists. While it does not oppose the concept of a watchlist per se, the practical use of such tools is fraught with peril for civil liberties. As currently administered, the no-fly list has spawned stigmatization, interrogation, delay, enhanced searches, detention and/or other travel impediments for innocent passengers. These innocent passengers can include prominent Americans such as Senator Ted Kennedy, who recently revealed that he was on the "no-fly" list for weeks, and people with the same name as terrorist suspects, such as the four innocent "David Nelsons" who were repeatedly stopped in the airport because their name

was on such a list. ACLU has filed a lawsuit seeking to vindicate the due process rights of people on the list. (www.aclu.org/nofly).

Expansion of the "no-fly" and "automatic selectee" lists, as proposed by the 9/11 Commission, should not go forward unless the TSA establishes adequate policies and procedures to ensure that the right people are on the list, people who are wrongly identified as terrorist suspects have a way of getting off of the list, and there is an independent review of the criteria used to put a person on one of the lists. The ombudsman process that the TSA has established has not to date proven adequate to accomplish these ends.

There is also some ambiguity in the report, which could result in parts of CAPPS II making their way into a reformed passenger screening system. Most notably, the commission's recommendations that the air carriers turn over all necessary information about their passengers to implement any new screening system could open the door to the same kinds of problems with the CAPPS II proposal. The TSA must not use this as an opening to engage in the dragnet screening of every air traveler. Suspicion must still be individualized, and based on reliable indicators of threat, not whimsy, bias or unproven profiling schemes.

Border Security and Immigration

Recommendation #19: While improved border security is important for national security, the report's "integrated approach" recommendation should not be implemented in a manner that creates what amounts to an "checkpoint society" or internal passport system. Discriminatory profiling should be rejected.

The 9/11 Commission recommended that the U.S. border security system be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. While border security screening needs to be improved, it should not be converted into a system of internal checkpoints at all major transportation systems.

Major transportation systems include trains, light rail, inter-city bus systems, intra-city bus systems, and subway systems such as the Metro system here in Washington, D.C. The process for boarding a Metro train should not be integrated into the system designed for those crossing the border. To do so would not only bring internal transportation to a crawl, but would fundamentally change the character of American society by creating a system of internal checkpoints. One should not have to scan a passport – or a federalized drivers license – to board a bus or hop on a subway train.

We do not believe that the 9/11 Commission meant to call for such a system, and we encourage members of the Commission to clarify this recommendation.

Rejection of discriminatory profiling and the "special registration" for visitors from Arab and Muslim countries. The 9/11 Commission essentially rejected any border security

scheme that singles visitors out based on national origin or other categorical criteria. None of its recommendations should be construed as supportive of any such system. The report says: "We advocate a system for screening, not categorical profiling. A screening system looks for particular, identifiable suspects or indicators of risk. It does not involve guesswork about who might be dangerous." (pg. 387).

We are hopeful that the Administration will interpret this recommendation in a way that ensures that the US VISIT program does not follow the path of its predecessor, the National Security Entry-Exit Registration System, or NSEERS. NSEERS singled young men visiting the United States from certain Muslim and Arab countries out for heightened scrutiny and forced them to register with the government; Congress should ensure that US VISIT does not go down this road.

Conclusion

Increased threats of terrorism after September 11, 2001, lightening-fast technological innovation, and the erosion of key privacy protections under the law threaten to alter the American way of life in fundamental ways. Terrorism threatens – and is calculated to threaten – not only our sense of safety, but also our freedom and way of life. Terrorists intend to frighten us into changing our basic laws and values and to take actions that are not in our long-term interests.

Proposals for fundamental reforms of the intelligence community are particularly sensitive because of the fundamental tension between intelligence gathering and civil liberties. Where government is focused on gathering intelligence information not connected to specific criminal activity, there is a substantial risk of chilling lawful dissent. Such inquiries plainly have a chilling effect on constitutional rights.

The answer is not to reject all intelligence and other reforms. The answer, instead, to ensure that specific safeguards for domestic collection of intelligence information that preserve the role of the FBI while ensuring against the use of spy tactics against Americans through strengthened guidelines and other checks to bar political spying. Greater openness, real accountability to both Congress and the public, and protection of whistleblowers is vitally necessary to challenge old assumptions and ensure better analysis and performance. If watch lists are used that have real consequences to those errantly on the list, then there must be a way to ensure that innocent people are not mistaken for dangerous ones, and to ensure that they can get off the list.

The 9/11 Commission should be applauded for avoiding the easy – and wrong – scapegoating of civil liberties and human rights protections for intelligence failures. The commissioners clearly understood that in order for America to remain strong and free, any reform of our intelligence or law enforcement communities must reflect the values and the ideals of our Constitution.

While we take exception to some of the 9/11 Commission's recommendations, such as the federalization of drivers licenses, we take heart from others, such as the call on government to justify broad expansions of power.

The challenge to our intelligence community is the same as the challenge to Congress, and for the nation as a whole. Securing the nation's freedom depends not on making a choice between security and liberty, but in designing and implementing policies that allow the American people to be both safe and free.

APPENDIX

9/11 Commission Recommendations
Summary of Civil Liberties Safeguards

National Intelligence Director, Counter-Terrorism Center must be accountable, not political

1. Intelligence director should not be White House official, but should be independent office, counter-terrorism center should not be in White House, and head of CIA should not be given more powers over domestic surveillance.

2. Intelligence director should be subject to Senate confirmation and should have a fixed term, like FBI Director and new Director of the CIA; President can fire for cause.

Make sure a "top cop," not a "top spy" remains in charge of domestic surveillance

3. Head of FBI intelligence operations must report to FBI Director and Attorney General, not intelligence chief;

4. FBI Director and Attorney General should be required to make and enforce guidelines prohibiting spying on First Amendment protected activity;

5. Powers of intelligence director and counter-terrorism center should be specified by statute, and other activities barred. Explicit, enforceable language should make clear intelligence director does not have effective control of domestic surveillance, whether directly or through counter terrorism-center.

6. No "covert operations" on American soil – use of domestic intelligence must be bound by legal system;

Reduce excessive secrecy, improve accountability

7. Create strong Inspector General and other internal watchdogs for intelligence community; create Civil Liberties Protection Board with real power to investigate abuses and prompt corrective action;

8. Restore presumption against classification for no good reason in prior Executive Order;

9. Amend Freedom of Information Act to provide that exemptions for new categories of unclassified, but nonpublic, information must be balanced against public interest in disclosure;

10. Enact legislation (e.g., S. 436/H.R. 2429) increasing public reporting on use of Foreign Intelligence Surveillance Act (FISA) that governs FBI national security wiretaps, secret searches, and records demands within United States;

11. Enact Lott-Wyden bill (S. 2672/H.R. 4855) establishing bipartisan classification review board, and make clear Senate is prepared to release information on board's recommendation if President is intransigent;

12. Intelligence committees must hold more open hearings, and open all legislative hearings;

13. Make intelligence budget public;

14. New and stronger committees to oversee intelligence community and Department of Homeland Security must allow for oversight by other relevant committees. Judiciary committees must have concurrent jurisdiction over domestic spying and other actions affecting constitutional rights.

15. Enact legislation (e.g., S. 2628/H.R. 3281) to provide specific protections for national security whistleblowers.

The USA Patriot Act

16. Congress should adopt the 9/11 Commission's framework for evaluating the USA PATRIOT Act, which puts the burden on the government to show a power is needed.

Border and Transportation Security

17. Congress should reject proposals to federalize drivers licenses and thereby turn them into a national ID that links databases and mandates immigration restrictions.

18. Standards for "no fly" and other watchlists must be enhanced to ensure there is clarity about how a person gets on a list, how the "same name" problem can be addressed, and how a person gets off.

19. Tracking "terrorist travel" should not be accomplished by a system of internal "checkpoints" that requires Americans to carry what amounts to an internal passport. Discriminatory profiling should be rejected.

Statement of Senator Joseph R. Biden, Jr.
Judiciary Committee Hearing on
The 9-11 Commission and Recommendations for the Future of
Federal Law Enforcement and Border Security
August 19, 2004

Mr. Chairman, Senator Leahy, thank you for calling this important hearing to examine several of the recommendations of the 9/11 Commission. Unfortunately, I am unable to attend today's session as I was previously committed to attend a biotechnology conference with the University of Delaware and the National Institutes of Health, but I would like to offer several observations on the matters before us.

The Commission makes several constructive suggestions for the FBI. I agree with all of them. But we should first pause to compliment the work of Director Mueller in this area, as the reforms he has put in place to redirect the FBI towards fighting and preventing acts of terror are largely blessed in the Commission's report. In May, I sat down with Director Mueller and outlined for him my view of the coming debate over the FBI's mission. We discussed the relative merits of the creation of a domestic security force along the lines of the British Security Service, or MI-5. I was impressed then with the Director's grasp both of the problems facing the Bureau, the concerns we both had about the MI-5 model, and the steps we both believed the Bureau should take to better prevent acts of terrorism while remaining the Nation's premier law enforcement agency. In June, in testimony in the other body, the Director outlined his vision for a new intelligence service within the FBI. I had indicated to Director Mueller in our May meeting that this sort of proactive, intelligent approach would counter those then calling for a wholesale creation of a new domestic security agency, and I am gratified to see the Commission endorse the Director's plan in their report. While more clearly needs to be done to reform the Bureau – its information needs to be better shared, its information technology systems still lag woefully behind, and its level of resources needs to be examined so that traditional crime-fighting needs do not go unmet – the suggestions made by the commissioners and the steps taken by Director Mueller are excellent ones.

Let me also compliment Asa Hutchinson in the job he is attempting to do at the Department of Homeland Security. We still miss him over at the DEA, but the work he and Secretary Ridge have undertaken is critical to our domestic security. I understand the Undersecretary's testimony today will focus largely on the border security efforts underway in his department; but I want to comment for a moment on the transportation security steps his agency is taking. At the outset, let me say that the Commission's observation that fully 90 percent of our transportation security resources have been dedicated to airline security – and that in so prioritizing we are effectively "fighting the last war", to use the Report's words – is both accurate and startling. I compliment Undersecretary Hutchinson for his efforts to secure the nation's air travel system, but the Administration's efforts on other modes of transportation have been sorely lacking.

What are we doing about rail security? Since 9/11, specific intelligence reports and official public warnings have confirmed that passenger rail systems in the United

States have been targeted by terrorists. Between 1997 and 2000, surface transportation systems worldwide were attacked 195 times by terrorists. Yet the Administration has requested no new authority to protect rail passengers. Since 9/11, and despite the terrible bombings in Madrid, the Administration has requested no new resources to protect rail passengers. Since 9/11, no new legislative authority to protect passenger rail has been passed by either the House or Senate. DHS has declined to fund Amtrak's priorities for improving security. As best I can tell, the only DHS actions to protect passenger rail in the wake of the Madrid attacks have been two pilot programs for screening passengers, one for sniffing explosives at the New Carrollton station and one for baggage screening at Union Station. A third pilot program will be the design and construction of a single new "smart car" with new security technologies – just one concept vehicle, not immediate actions that could enhance security.

Amtrak itself has been historically underfunded – it does not have the funds to undertake substantial security upgrades on its own, and it needs significantly more federal dollars to secure its rails. More people pass through Penn Station in New York City every day than through all three major New York airports. The fact is that Amtrak, carrying just intercity traffic, logs 23 million passenger miles a year. In May of this year, *National Journal* asked security experts to rank the efforts of the Department of Homeland Security. Rail security came in dead last, with a failing score of 1.6 out of a possible 5. I am well aware that securing the trains is difficult – it is an essentially open system, connected to mass transit and commuter rail systems in every city, and it is unlike the sealed systems we create around airports. But there are obvious, simple, easy and effective first steps we can take to make our rail system much safer: improve lighting; install blast-resistant trash cans; add closed circuit TV cameras; increase public awareness of security threats such as unattended baggage; increase the numbers of rail security personnel. This Administration has chosen to do none of them. In fact, DHS has been shown Amtrak's priorities for improving security, and has declined to fund Amtrak requests for assistance.

So when the Commission reports that we are "fighting the last war" when it comes to transportation security, I could not agree more. I also agree with their recommendation that DHS develop an integrated plan to focus resources in a manner to best protect all the transportation modes. It is intolerable that such a plan has not been developed and put in place already, and I call on Secretary Ridge to develop an infrastructure protection plan and submit it to Congress for our consideration within the next ninety days.

Finally, let me take a moment to comment on a subject that I understand is not necessarily a topic of this morning's hearing, but one that I fear is getting lost in the debate over appropriate post-9/11 improvements: our state and local law enforcement agencies. The heroes of 9/11 – the New York City cop, the local law enforcement officer – are being shortchanged by this Administration. We have not put one new cop on the street since those terrible attacks. Studies indicate police departments across the country are being forced to lay off officers due to budgetary constraints. The war in Iraq has resulted in the depletion of many cities' and towns' police forces. The President insists

upon ending the COPS program, the one Washington-based initiative proven to have helped lower crime rates. Mindless budget cutting at the Department of Justice is threatening our public safety and homeland security efforts, to the point where police chiefs throughout the country have labeled the Administration's plans unacceptable.

We should be doing exactly the opposite. We should be infusing a refocused COPS program with new resources, resources to help police department build their intelligence units, add officers to the streets, and in so doing assist the FBI and DHS prevent the next attack. Just yesterday, the *Washington Times* published an editorial by a Brookings Institute fellow calling for a "COPS II" to efficiently beef up local police anti-terrorism units. I agree with this proposal, and reiterate my call for a dramatic boost in local law enforcement spending so we can truly help our first responders -- our cops on the street -- prevent the next attack.

Mr. Chairman, I thank you again for calling this critical hearing. I look forward to reviewing the record of today's proceeding, and to working with you to implement the effective recommendations of the 9/11 Commission.

STATEMENT OF

MAUREEN A. BAGINSKI
EXECUTIVE ASSISTANT DIRECTOR
INTELLIGENCE

FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
SENATE COMMITTEE ON THE JUDICIARY

August 19, 2004

Introduction

Good afternoon, Chairman Hatch and Members of the Committee. It is my pleasure to come before you today to discuss the recommendations of the 9-11 Commission, specifically those involving the Federal Bureau of Investigation. As Director Mueller has said, the FBI has worked closely with the Commission and their staff throughout their tenure and we commend them for an extraordinary effort. Throughout this process, we have approached the Commission's inquiry as an opportunity to gain further input from outside experts. We took their critiques seriously, adapted our ongoing reform efforts, and have already taken substantial steps to address their remaining concerns. We are gratified and encouraged that the Commission has embraced our vision for change and has recognized the progress that the men and women of the FBI have made to implement that vision. Our work to date has been on strengthening FBI capabilities so that we can be a strong node on the information network of those who defend the nation. Vital information about those who would do us harm is not produced by the federal government alone. We are proud to also be part of an 800,000 strong state, local, and tribal law enforcement community who are the first to encounter and defend against threats.

As you are aware, the terrorist threat of today represents complex challenges. Today's terrorists operate seamlessly across borders and continents, aided by sophisticated communications technologies; they finance their operations with elaborate funding schemes; and they patiently and methodically plan and prepare their attacks. To meet and defeat this threat, the FBI must have several critical capabilities:

- First, we must be intelligence-driven. To defeat the terrorists, we must develop intelligence about their plans and use that intelligence to disrupt those plans.
- We must be global. We must continue our efforts to develop our overseas law enforcement efforts, our partnerships with foreign law enforcement,

and our knowledge and expertise about foreign cultures and our terrorist adversaries overseas.

- We must have networked information technology systems. We need the capacity to manage and share our information effectively.
- Finally, we must remain accountable under the Constitution and the rule of law. We must respect civil rights and civil liberties as we protect the American people.

To achieve success in this war on terror, we have transformed the FBI's Counterterrorism (CT) program and integrated our investigative and intelligence operations; we have improved information sharing with other federal agencies and state and local law enforcement entities; and enhanced our operational capabilities within FBIHQ and all local Field Offices. Under the direction of Director Mueller, the FBI has moved aggressively forward in this regard by implementing a comprehensive plan that has fundamentally transformed the FBI. The FBI today has a clear hierarchy of national priorities with the prevention of terrorist attacks at the top. These priorities have been institutionalized throughout the FBI.

On August 2nd, the President announced his intention to establish a National Intelligence Director (NID) and a National Counter Terrorism Center (NCTC). We look forward to working with you on these vital reforms.

Our core guiding principle at the FBI is that intelligence and law enforcement operations must be integrated. A prerequisite for any operational coordination is the full and free exchange of information. Without procedures and mechanisms that allow information sharing on a regular and timely basis, we and our partners cannot expect to align our operational efforts to best accomplish our shared mission. Accordingly, we have taken steps to establish unified FBI-wide policies for sharing information and intelligence both within the FBI and outside it. This has occurred under the umbrella of the FBI's Intelligence Program, and is my personal responsibility as the FBI executive for information sharing. We have made great progress and we have much work ahead of us.

Intelligence Program

The mission of the FBI's Intelligence Program is to optimally position the FBI to meet current and emerging national security and criminal threats by (1) aiming core investigative work proactively against threats to US interests, (2) building and sustaining enterprise-wide intelligence policies and human and technical capabilities, and (3) providing useful, appropriate, and timely information and analysis to the national security, homeland security, and law enforcement communities. Building on already strong FBI intelligence capabilities, Director Mueller created in January 2003 the position of Executive Assistant Director (EAD) of Intelligence and an Office of Intelligence. I was honored to join the FBI in May 2003 as the first EAD Intelligence.

Core Principles

We built the FBI Intelligence Program on the following core principles:

- *Independent Requirements and Collection Management*: While intelligence collection, operations, analysis, and reporting are integrated at headquarters divisions and in the field, the Office of Intelligence manages the requirements and collection management process. This ensures that we focus intelligence collection and production on priority intelligence requirements and on filling key gaps in our knowledge.

- *Centralized Management and Distributed Execution:* The power of the FBI intelligence capability is in its 56 field offices, 400 resident agencies and 56 legal attaché offices around the world. The Office of Intelligence must provide those entities with sufficient guidance to drive intelligence production effectively and efficiently, but not micro-manage field intelligence operations.

- *Focused Strategic Analysis:* The Office of Intelligence sets strategic analysis priorities and ensures they are carried out both at headquarters and in the field. This is accomplished through a daily production meeting that I chair.

- *Integration of Analysis with Operations*: Intelligence analysis is best when collectors and analysts work side-by-side in integrated operations.

Concept of Operations

Concepts of Operations (CONOPs) guide FBI intelligence processes and detailed implementation plans drive specific actions to implement them. Our CONOPs cover the following core functions: *Intelligence Requirements and Collection Management; Intelligence Assessment Process; Human Talent for Intelligence Production; Field Office Intelligence Operation; Intelligence Production and Use; Information Sharing; Community Support; Threat Forecasting and Operational Requirements; and Budget Formulation for Intelligence.*

Accomplishments

What follows are some of our key accomplishments:

- We have issued the first-ever FBI requirements and collection tasking documents. These documents are fully aligned with the DCI's National Intelligence Priorities Framework and we have published unclassified versions for our partners in state, local, and tribal law enforcement.

- We are full members of the National Intelligence Collection Board and the National Intelligence Analysis and Production Board, and soon will be participating in the drafting of National Intelligence Estimates and the National Foreign Intelligence Board.

- We have created a collection capabilities database that tells us what sources we can bring to bear on intelligence issues across the FBI.

- We have created FBI homepages on INTELINK, SIPRNET, and Law Enforcement Online (LEO) for dissemination and evaluation of our intelligence product.

- We have established a daily Intelligence Production Board to ensure that timely decisions are made regarding the production and dissemination of all analytical products. The Board reviews the significant threats, developments, and issues emerging in each investigative priority area, and identifies topics for intelligence products.

- We have completed the first-ever FBI intelligence dissemination manual.

- We have proposed and are building an Intelligence Officer certification program for Agents, Analysts, Surveillance Specialists and Language Analysts. Once established this certification will be a pre-requisite for advancement to Section Chief or Assistant Special Agent in Charge, thus ensuring that all FBI senior managers will be fully trained and experienced intelligence officers.

- We have completed and begun to implement the CONOPs for Intelligence Analysts. We have set unified standards, policies, and training for intelligence analysts. In a new recruiting program veteran analysts are attending events at colleges and universities throughout the country and we are offering hiring bonuses to analysts for the first time in FBI history.

- We are in the process of changing the criteria on which Agents are evaluated to place more emphasis on intelligence-related function.

- We are on course to triple our intelligence production this year.

- We have placed reports officers in our Joint Terrorism Task Forces (JTTFs) to ensure vital information is flowing to those who need it.

- We have developed detailed metrics to judge the results of our intelligence initiatives and are prepared to regularly report performance and progress to Congress and other stakeholders, partners, and customers.

- We have established Field Intelligence Groups (FIGs) to integrate analysts, Agents, linguists, and surveillance personnel in the field to bring a dedicated team focus to intelligence operations. As of June 2004, there are 1,450 FIG personnel, including 382 Special Agents and 160 employees from other Government agencies. Each FIG is under the direct supervision of an Assistant Special Agent in Charge.

- From October 2003 to April 2004, the FBI participated in more than 10 recruitment events and plans to add at least five additional events through September 2004. A marketing plan also was implemented to attract potential candidates. In February 2004, an advertisement specific to the Intelligence Analyst position at the FBI was placed in *The Washington Post*, *The Washington Times*, and the *New York Times*, and has since been run several more times. Our National Press Office issued a press release that kicked off an aggressive hiring campaign.

- The College of Analytic Studies (CAS), established in October 2001, is based at the FBI Academy in Quantico, Virginia. Since FY 2002, 264 analysts have graduated from the College's six-week Basic Intelligence Analyst Course. 655 field and headquarters analysts have attended specialty courses on a variety of analytical topics. 1,389 field and headquarters employees have attended specialized counterterrorism courses offered in conjunction with CIA University, and 1,010 New Agent Trainees have received a two-hour instructional block on intelligence.

- The Basic Intelligence Course currently offered by the CAS is being revised and updated to incorporate key elements of our intelligence program. Upon completion of this effort, the course will be retitled: Analytical Cadre Education Strategy I (ACES I) as outlined in the Human Talent CONOPS. An intermediate course entitled ACES II is anticipated in the future that would target more experienced analysts. Practical exercises and advanced writing skills will be emphasized, as well as advanced analytical techniques.

- The ACES I course will incorporate seven core elements of intelligence relevant for new agents and new analysts. Additionally ACES I will focus on assimilation, analytic tradecraft and practice, thinking and writing skills, resources, and field skills.

- Complementing ACES I and ACES II, the Office of Intelligence, in coordination with the FBI Training and Development Division, will identify, facilitate, and

exploit training partnerships with other government agencies, academia, and the private sector to fully develop the career choices of FBI analysts. Whether an analyst chooses the specialized, interdisciplinary, or managerial career path, s/he will have the opportunity to attend courses offered through the Joint Military Intelligence Training Center, other government training centers, and private companies.

- The Office of Intelligence is also establishing education cooperative programs where college students will be able to work at the FBI while earning a four-year degree. Students may alternate semesters of work with full-time study or may work in the summers in exchange for tuition assistance. In addition to financial assistance, students would benefit by obtaining significant work experience, and the FBI would benefit through an agreement requiring the student to continue working for the FBI for a specific period of time after graduation. This program will be implemented in FY 2005.

- An Analyst Advisory Group has also been created specifically to address analytical concerns. I established and chair the advisory group - composed of Headquarters and field analysts. The group affords analysts the opportunity to provide a working-level view of analytic issues and to participate in policy and procedure formation. They are involved in developing promotional criteria, providing input for training initiatives, and establishing the mentoring program for new FBI analysts.

- The Career Mentoring Working Group of the Analyst Advisory Group is creating a career mentoring program to provide guidance and advice to new analysts. Once implemented, all new Intelligence Analysts will have a mentor to assist them. The career mentor will have scheduled contact with the new analyst on a monthly basis throughout the analyst's first year of employment.

- As of this year, the Director's Awards will feature a new category: the Director's Award for Excellence in Intelligence Analysis. Nominees for this award must display a unique ability to apply skills in intelligence analysis in furtherance of the FBI's mission, resulting in significant improvements or innovations in methods of analysis that contribute to many investigations or activities, and/or overcoming serious obstacles through exceptional perseverance or dedication leading to an extraordinary contribution to a significant case, program, threat, or issue.

- Turning to intelligence training for our agents, we are now working to incorporate elements of our basic intelligence training course into the New Agents Class curriculum. We expect that work to be completed by September. A key element of this concept is that agents in New Agents Training and analysts in the College of Analytic Studies will conduct joint training exercises in intelligence tradecraft. The first offerings to contain these joint exercises are expected in December of this year. In addition to this, we are in the process of changing the criteria on which agents

are evaluated to place more emphasis on intelligence-related functions and information sharing.

- On March 22, 2004, Director Mueller also adopted a proposal to establish a career path in which new Special Agents are initially assigned to a small field office and exposed to a wide range of field experiences. After approximately three years, agents will be transferred to a large field office where they will specialize in one of four program areas: Intelligence, Counterterrorism/ Counterintelligence, Cyber, or Criminal, and will receive advanced training tailored to their area of specialization. In our Special Agent hiring, we have changed the list of "critical skills" we are seeking in candidates to include intelligence experience and expertise, foreign languages, and technology.

- Our language specialists are critical to our intelligence cadre as well. The FBI's approximately 1,200 language specialists are stationed across 52 field offices and headquarters, and are now connected via secure networks that allow language specialists in one FBI office to work on projects for any other office. Since the beginning of FY 2001, the FBI has recruited and processed more than 30,000 linguist applicants. These efforts have resulted in the addition of nearly 700 new linguists with a Top Secret security clearance. In addition, the FBI formed a Language Services Translation Center to act as a command and control center to coordinate translator assignments and maximize its capacity to render immediate translation assistance.

Information Sharing

The FBI shares intelligence with other members of the Intelligence Community, to include the intelligence components of the Department of Homeland Security (DHS), through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include both raw and finished intelligence reports. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins. To support information sharing, there is now a Special Agent or Intelligence Analyst in the JTTFs dedicated to producing "raw" intelligence reports for the entire national security community, including state, municipal, and tribal law enforcement partners and other JTTF members. These reports officers are trained to produce intelligence reports that both protect sources and methods and maximize the amount of information that can be shared. It is the responsibility of the FIGs to manage, execute, and maintain the FBI's intelligence functions within the FBI field office. FIG personnel have access to TS and SCI information so they will be able to receive, analyze, review and recommend sharing this information with entities within the FBI as well as our customers

and partners within the Intelligence and law enforcement communities.

We have also worked closely with DHS to ensure that we have the integration and comprehensive information sharing between our agencies that are vital to the success of our missions. The FBI and DHS share database access at TTIC, in the National JTTF at FBI Headquarters, in the Foreign Terrorist Tracking Task Force (FTTTF) and the Terrorist Screening Center (TSC), and in local JTTFs in our field offices around the country. We worked closely together to get the new Terrorist Screening Center up and running. We hold weekly briefings in which our Counterterrorism analysts brief their DHS counterparts on current terrorism developments. The FBI and DHS now coordinate joint warning products to address our customers' concerns about multiple and duplicative warnings. We designated an experienced executive from the Transportation Security Administration to run the TSC, a DHS executive to serve as Deputy Director of the TSC, and a senior DHS executive was detailed to the FBI to ensure coordination and transparency between the agencies.

The FBI has a responsibility to the nation, Intelligence Community, and federal, state, and local law enforcement to disseminate information, and to do so is an inherent part of our mission. Sharing FBI information will be the rule, unless sharing is legally or procedurally unacceptable.

Next Steps

With our counterterrorism and intelligence initiatives, we have made great progress, but we have much work to do. Our plan is solid and we believe we are heading in the right direction. We have enjoyed much support from your committee and we are very appreciative of the time your staff has spent in learning about our initiatives and giving us advice. What we need more than anything else is your continued support and understanding that a change of this magnitude will require time to implement. With your help, we will have that. Thank you for allowing me the opportunity to testify before you today and I will be happy to entertain any questions you may have.

Sen Saxby Chambliss
Insert for the Record

FACT SHEET: KEY BUSH ADMINISTRATION ACTIONS CONSISTENT WITH 9/11 COMMISSION RECOMMENDATIONS

President Bush welcomes the 9/11 Commission report and agrees with its conclusion that our Homeland is safer today, but we are not yet safe. He has ordered the highest levels of government to examine in short order the Commission's recommendations and to use them to develop a plan for further action.

The Commission carefully and thoughtfully studied the many complex and critical issues facing our Nation in the War on Terror – and we are gratified that the Commission's final report comes to conclusions similar to the Administration's on the vast majority of the key policy issues.

As the Commission recommended:

- **The Administration is already pursuing a worldwide strategy of disrupting and denying safe harbors to terrorist groups.** We continue to build on these efforts, and the Administration is giving serious consideration to the Commission's recommendations.
- **The Administration is already undercutting the ideological appeal of terrorism by standing for a "forward strategy of freedom" and promoting needed reforms in the broader Middle East.** The Administration welcomes the Commission's recommendations for further strengthening and expanding these efforts.
- The Administration **is already developing and deploying cutting-edge technologies to secure our borders, our ports, our critical infrastructure,** and other parts of our homeland. Although there is no such thing as perfect security in our vast, free Nation, the Administration believes more can be done to build on the efforts we have begun, and the Commission's homeland security recommendations are being seriously reviewed.
- **The Administration has already moved significantly along the road to intelligence reform** by vastly improving cooperation and information-sharing among the intelligence, law enforcement, and homeland security communities through:
  - passage of the USA PATRIOT Act;
  - the ongoing transformation of the FBI;
  - expansion of the collection and analytical capabilities of CIA; and
  - creation of the Department of Homeland Security, the Terrorist Threat Integration Center, and the Terrorist Screening Center.

  These are important steps along the road the Commission charts for intelligence reform. More steps are needed – and more will be taken – but a solid foundation for future action is in place. The Commission's intelligence-reform proposals build on this foundation. The reform efforts we take now will establish an intelligence structure to protect America for decades to come, and it is important to get it right, which is why the Administration is actively and seriously examining each of the Commission's recommendations.

The following are examples of actions already taken by the Bush Administration that are fulfilling the 9/11 Commission's recommendations.

RECOMMENDATIONS	ACTIONS ALREADY TAKEN
Chapter 12 "What To Do? A Global Strategy"	
➢ "The U.S. government must identify and prioritize actual or potential terrorist sanctuaries. For each, it should have a realistic strategy to keep possible terrorists insecure and on the run, using all elements of national power. We should reach out, listen to, and work with other countries that can help." (Ch. 12, p. 367)	➢ *The removal of all al Qaeda sanctuaries was part of our strategy before 9/11. Since 9/11, the United States has removed the #1 terrorist sanctuary, the Taliban regime in Afghanistan, and also Saddam Hussein's regime in Iraq, a long-time state sponsor of terror. We continue to use all elements of national power to identify and eliminate other such sanctuaries around the world and to work with other governments to make sure they are not available to terrorists. We are destroying the leadership of terrorist networks; disrupting their planning and financing; and shrinking the space in which they can freely operate by denying them territory and the support of governments. The effort to identify and eliminate terrorist sanctuaries is ongoing and will continue to be a central element of our strategy in the War on Terror.*
➢ "If Musharraf stands for enlightened moderation in a fight for his life and for the life of his country, the United States should be willing to make hard choices too, and make the difficult and long-term commitment to the future of Pakistan. Sustaining the current scale of aid to Pakistan, the United States should support Pakistan's government in its struggle against extremists with a comprehensive effort that extends from military aid to support for better education, so long as Pakistan's leaders remain willing to make the difficult choices of their own." (Ch. 12, p. 369)	➢ *The United States has dramatically re-fashioned its relationship with Pakistan in the wake of the 9/11 attacks. As the Commission notes, even before 9/11, the Bush Administration was actively engaged in diplomatic efforts to get Pakistan to change its policy of support for the Taliban and help eliminate the al Qaeda threat. President Bush personally wrote President Musharraf in February 2001 emphasizing that Bin Ladin and al Qaeda were a "direct threat the United States and its interest that must be addressed" and urging Musharraf to use his influence with the Taliban on this critical issue. Again in August 2001, President Bush personally asked Musharraf for Pakistan's active engagement against al Qaeda. Today, the United States and Pakistan are working closely in the fight against terror, and Pakistani forces are rounding up terrorists along their nation's western border. President Musharraf is a friend of our country, and has taken out of commission over 500 al Qaeda and Taliban operatives, including Khalid Sheik Mohammed, the operational planner behind the 9/11 attacks. Finally, we have proposed a five-year, $3 billion military and aid package to support Pakistan's security, economic and social programs.* ➢ *American assistance to help improve the lives of Pakistanis will reach $300 million for the period of 2002 to 2006. Improvements to primary and secondary education, modernization of health care – especially for women and children – and helping small and medium Pakistani businesses compete in the international market are some areas in which Pakistanis and Americans are working together. This year alone, 130 schools are being refurbished, a program to reduce maternal and infant mortality is being launched, and scholarships are being given to top students who could not otherwise afford to go to Pakistani universities.*

➢ "The President and the Congress deserve praise for their efforts in Afghanistan so far. Now the United States and the international community should make a long-term commitment to a secure and stable Afghanistan, in order to give the government a reasonable opportunity to improve the life of the Afghan people. Afghanistan must not again become a sanctuary for international crime and terrorism. The United States and the international community should help the Afghan government extend its authority over the country, with a strategy and nation-by-nation commitments to achieve their objectives." (Ch. 12, p. 370)	➢ *The United States and its coalition partners defeated the Taliban, put al Qaeda on the run and eliminated Afghanistan as the international hub for al Qaeda terrorist training. This Administration committed $2 billion for Afghanistan's development. Today, Afghans have a new stable currency, a new Constitution, and are looking forward to voting in the country's first democratic elections. The United States has reassured the Afghan government that America is a steadfast partner. The UN and international community have also pledged to ensure Afghanistan does not plunge into anarchy. To ensure security and stability, the United States and the international community are training security forces to extend Kabul's authority in the provinces. Currently there are over 13,000 soldiers in the well-respected Afghan National Army and over 21,000 Police officials. In addition, the United Kingdom and the United States are better positioning themselves to counter a growing narcotics threat now and over the long-term. Reconstruction programs such as completing the Kabul to Kandahar road; continuing work on the Kabul to Herat road and secondary roads; building clinics and schools; training teachers; and establishing market centers all contribute to a stable and secure Afghanistan.*
➢ "The problems in the U.S.-Saudi relationship must be confronted, openly. The United States and Saudi Arabia must determine if they can build a relationship that political leaders on both sides are prepared to publicly defend—a relationship about more than oil. It should include a shared commitment to political and economic reform, as Saudis make common cause with the outside world. It should include a shared interest in greater tolerance and cultural respect, translating into a commitment to fight the violent extremists who foment hatred." (Ch. 12, p. 374)	➢ *Three years ago, terrorists were well established in Saudi Arabia. Inside that country, fundraisers and other facilitators gave al Qaeda financial and logistical help – with little scrutiny or opposition. Today, after attacks in Riyadh and elsewhere, the Saudi government knows that al Qaeda is its enemy. Saudi Arabia is working hard to shut down the facilitators and financial supporters of terrorism, and has captured or killed many first-tier leaders of the al Qaeda organization in Saudi Arabia – including one in June 2004. Today, because Saudi Arabia has seen the danger, and has joined the War on Terror, the American people are safer. While there is still much work to be done, the Saudis have made important progress in confronting the terrorist threat and the United States has forged a genuine partnership with Saudi Arabia in this war, one that will continue to pay dividends in the years ahead.*

➢ "The U.S. government must define what the message is, what it stands for. We should offer an example of moral leadership in the world, committed to treat people humanely, abide by the rule of law, and be generous and caring to our neighbors. America and Muslim friends can agree on respect for human dignity and opportunity. To Muslim parents, terrorists like Bin Ladin have nothing to offer their children but visions of violence and death. America and its friends have a crucial advantage–we can offer these parents a vision that might give their children a better future. If we heed the views of thoughtful leaders in the Arab and Muslim world, a moderate consensus can be found." (Ch. 12, p. 376)	➢ *In Afghanistan and Iraq, the United States is leading international coalitions to help citizens build a democratic future. Free and fair national elections will be held for the first time in Afghanistan this October, and in Iraq by the end of January. Last June, President Bush led the G-8 Leaders in launching the "Partnership for Progress and a Common Future" to support political, economic, and social reform in the Broader Middle East and North Africa region by committing to: establish a Forum for the Future, bring together regularly G-8 and regional ministers to discuss reforms and support progress in the region; bring together democracy foundations, civil society groups, and governments from the G-8, the region, and other countries to promote and strengthen democratic institutions, coordinate and share information on democracy programs, initiate new democracy programs, and sponsor exchanges; assist the region's efforts to halve the illiteracy rate over the next decade, including by training 100,000 teachers by 2009; help as many as 250,000 young entrepreneurs, especially women, expand their employment opportunities; invest $100 million to assist small and medium-sized enterprises; expand sustainable microfinance in the region to help over two million potential small entrepreneurs pull themselves out of poverty; coordinate the work of development institutions and international financial institutions working in the region; and assist the region's efforts to improve the business climate.*
➢ "Where Muslim governments, even those who are friends, do not respect these principles, the United States must stand for a better future. One of the lessons of the long Cold War was that short-term gains in cooperating with the most repressive and brutal governments were too often outweighed by long-term setbacks for America's stature and interests." (Ch. 12, p. 376)	➢ *The President has embedded democracy, transparency, and respect for the rule of law into the core of our foreign policy and assistance strategies. A few examples of this fundamental commitment include:* o *The Millennium Challenge Account (MCA). At the Inter-American Development Bank on March 14, 2002, President Bush called for "a new compact for global development, defined by new accountability for both rich and poor nations alike. Greater contributions from developed nations must be linked to greater responsibility from developing nations." The President pledged that the United States would lead by example and increase its core development assistance by 50 percent over the next three years, resulting in an annual increase of $5 billion by FY 2006;* o *The Middle East Partnership Initiative, which is based on the President's conclusion that we must never seek "stability" at the price of freedom; and* o *The Anti-Corruption efforts in the G-8, Asia Pacific Economic Cooperation (APEC), and Summit of the Americas.*

"Just as we did in the Cold War, we need to defend our ideals abroad vigorously. America does stand up for its values. The United States defended, and still defends, Muslims against tyrants and criminals in Somalia, Bosnia, Kosovo, Afghanistan, and Iraq. If the United States does not act aggressively to define itself in the Islamic world, the extremists will gladly do the job for us." (Ch. 12, p. 377)	*President Bush is committed to the long-term future of Afghanistan and Iraq, two nations in the midst of historic transitions from dictatorship to democracy. On November 6, 2003, the President announced the Forward Strategy of Freedom in the Broader Middle East, which is a vision based on the President's conclusion that we must never seek "stability" at the price of freedom. The President's Broader Middle East Initiative, endorsed at the G-8, US/EU, and NATO summits in June 2004, is rooted in a partnership to support the region's aspirations for freedom, democracy, rule of law, economic opportunity, and social justice. The partnership involves not only governments, but also business and civil society leaders as full partners.*
"The U.S. government should offer to join with other nations in generously supporting a new International Youth Opportunity Fund. Funds will be spent directly for building and operating primary and secondary schools in those Muslim states that commit to sensibly investing their own money in public education." (Ch. 12, p. 378)	*Promoting literacy and developing new opportunities for young people in the Broader Middle East region are key priorities underpinning the President's Broader Middle East and North Africa initiative. The President led the G-8 at the Sea Island Summit in launching new initiatives to support the region's literacy efforts and sponsor entrepreneurship and vocational training programs. Internationally, the President has more than tripled U.S. overseas basic education funding.*
"A comprehensive U.S. strategy to counter terrorism should include economic policies that encourage development, more open societies, and opportunities for people to improve the lives of their families and to enhance prospects for their children's future." (Ch. 12, p. 379)	*In an unparalleled manner, the President has united aid and trade policies to help integrate the poorest countries into the global economy in a way that promotes free, democratic, and prosperous societies. Examples include the Millennium Challenge Account (MCA), the Digital Freedom Initiative, the Trade for African Development and Enterprise (TRADE) initiative, the Middle East Partnership Initiative, the Africa Growth and Opportunity Act (AGOA) II and III, and an unprecedented number regional, sub-regional, and bilateral free trade agreements that the Administration is negotiating or has concluded with developing countries. This includes a Presidential initiative to establish a U.S.-Middle East Free Trade Area (MEFTA) by 2013. The recently passed U.S.-Morocco FTA, completion of FTA negotiations with Bahrain, and the signing of Trade and Investment Framework Agreements with every country in the Arabian Gulf demonstrate concrete progress toward the MEFTA goal. Finally, the Administration provided a critical global leadership in successfully launching the WTO's Doha Development Agenda trade negotiations -- the first round of global trade talks focused on developing country development.*

➢ "The United States should engage other nations in developing a comprehensive coalition strategy against Islamist terrorism. There are several multilateral institutions in which such issues should be addressed. But the most important policies should be discussed and coordinated in a flexible contact group of leading coalition governments. This is a good place, for example, to develop joint strategies for targeting terrorist travel, or for hammering out a common strategy for the places where terrorists may be finding sanctuary" (Ch. 12, p. 379)	➢ *In addition to our bilateral counterterrorism (CT) relationships with key partners around the world, the United States has sought to advance an aggressive CT agenda in numerous multilateral fora, such as NATO, the APEC forum, and the G-8, where the President led leaders in June 2003 in establishing a dedicated group of donor countries to expand and coordinate training and assistance for weak but willing countries. Other organizations, including the Organization of American States (OAS), the European Union (EU), the Association of South East Asian Nations (ASEAN), and the Australia, New Zealand, and United States (ANZUS) Treaty members took concrete steps to combat terrorism more effectively and to cooperate with each other to address this transnational threat. Reorienting existing partnerships and developing multilateral solutions to the threat remains an essential part of our strategy to win the War on Terror.*
➢ "The United States should engage its friends to develop a common coalition approach toward the detention and humane treatment of captured terrorists. New principles might draw upon Article 3 of the Geneva Conventions on the law of armed conflict. That article was specifically designed for cases in which the usual laws of war did not apply. Its minimum standards are generally accepted throughout the world as customary international law." (Ch. 12, p. 380)	➢ *The United States has worked closely with its coalition partners regarding the detention and treatment of captured terrorists, and is open to exploring whether a "common coalition approach" is feasible and consistent with our national security.*

"Our report shows that al Qaeda has tried to acquire or make weapons of mass destruction for at least ten years. There is no doubt the United States would be a prime target. Preventing the proliferation of these weapons warrants a maximum effort—by strengthening counterproliferation efforts, expanding the Proliferation Security Initiative, and supporting the Cooperative Threat Reduction program." (Ch. 12, p. 381)	*Since publishing the National Strategy to Combat Weapons of Mass Destruction in 2002, this Administration has fundamentally changed the way our Nation responds to this threat. For example, we have:* ○ *eliminated the WMD programs and SCUD-C missiles in Libya;* ○ *brought to a close Saddam Hussein's decades-long pursuit of chemical, biological, and nuclear weapons;* ○ *closed down the A.Q. Khan nuclear proliferation network;* ○ *achieved the unanimous passage of UNSCR 1540 that requires states to enact legislation that criminalizes proliferation activities;* ○ *established 'Biodefense for the 21st Century,' a national strategy for meeting the full range of biological threats;* ○ *provided record-level resources devoted to Nunn-Lugar and other nonproliferation assistance, including through the creation of the G-8 Global Partnership, which will provide $20 billion to this effort over 10 years;* ○ *signed into law Project BioShield, which provides new tools to improve medical countermeasures protecting Americans against a chemical, biological, radiological, or nuclear (CBRN) attack; and* ○ *established the Proliferation Security Initiative (PSI), a broad international partnership of countries to coordinate actions to interdict proliferation shipments of WMD and related materials – at sea, in the air, and on land – and to shut down proliferation networks and entities.*

"Vigorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us to understand their networks, search them out, and disrupt their operations. Intelligence and law enforcement have targeted the relatively small number of financial facilitators—individuals al Qaeda relied on for their ability to raise and deliver money—at the core of al Qaeda's revenue stream. These efforts have worked. The death or capture of several important facilitators has decreased the amount of money available to al Qaeda and has increased its costs and difficulty in raising and moving that money. Captures have additionally provided a windfall of intelligence that can be used to continue the cycle of disruption." (Ch. 12, p. 382)	*In the war on terrorist financing we have successfully disrupted and, in some cases, dismantled the financial infrastructure of terrorist operations. Working in cooperation with the international community, we have frozen more than $140 million in terrorist-related assets, designated 383 individuals and entities as terrorist supporters, apprehended or disrupted key terrorist facilitators and deterred donors from supporting al Qaeda and other like-minded terrorist groups. America is safer today because we have made it harder and costlier for al Qaeda and other terrorist groups to raise and move money around the world.* *The Administration has collaborated with Congress to develop a new Treasury Department structure to strengthen our efforts to fight terrorist financing. The Office of Terrorism and Financial Intelligence (TFI) will bring together Treasury's intelligence, regulatory, law enforcement, sanctions, and policy components in a high-profile effort led by an Under Secretary and two Assistant Secretaries.*
"Targeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility." (Ch. 12, p. 385)	*We have already undertaken numerous post-9/11 initiatives that significantly enhance security with respect to travelers to the United States. Consular interviews of visa applicants are much more rigorous and utilize a larger database of terrorism-related information. Applications of concern are referred to Washington for in-depth review through the Security Advisory Opinion (SAO) process. Incoming international air travelers are subject to comprehensive prescreening carried out by the new National Targeting Center (NTC). When travelers reach U.S. ports of entry, the new Customs and Border Protection (CBP) agency conducts integrated "one face at the border" inspections. Watch lists are being consolidated through the Terrorist Screening Center (TSC) and the Terrorist Threat Integration Center (TTIC). These, and many other US intelligence analysis capabilities, are being used to attempt to exploit terrorists' vulnerabilities as they travel and to learn more about their activities and methods. The US-VISIT entry-exit system uses biometrics to compare the identity of the traveler with known data.* *In addition to our ongoing efforts to target terrorist travel to, from and within the United States, the Administration is seeking, on both a bilateral and multilateral basis, to promote similar efforts by other responsible governments, and to provide those governments with relevant terrorist-related information.*

➢ "The U.S. border security system should be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with the systemwide goals in mind. Extending those standards among other governments could dramatically strengthen America and the world's collective ability to intercept individuals who pose catastrophic threats." (Ch. 12, p. 387)	➢ *The Administration has made great progress in implementing an improved homeland security strategy that relies extensively on a "layered" approach to screening that actually begins well beyond U.S. borders.* o *The comprehensive screening process begins with the careful review of all visa applications by consular officers overseas, who now have ready access to extensive databases with terrorism-related information.* o *New Federal Regulations require traveler and cargo information to be provided to U.S. authorities before arrival in the United States.* o *The Container Security Initiative allows U.S. inspectors at 17 major foreign seaports to examine high-risk containers before they are placed on U.S.-bound ships.* o *Three years ago, there were inspectors from three different Federal agencies at our ports of entry. Today, through DHS, the Bureau of Customs and Border Protection (CBP) consolidates not only all of our border inspectors, but also those who patrol between the ports of entry to create "one face at the border."* o *The Administration is working with other governments on transportation security, including through detailed action plans for implementing Border Accords with Canada and Mexico. The U.S.-introduced Secure and Facilitated International Travel Initiative (SAFTI), announced at the recent G-8 Summit at Sea Island, Georgia, constitutes a redoubled commitment by G-8 countries to a coordinated, comprehensive strategy to move travelers (and goods) across international borders quickly and easily, while providing enhanced security procedures.*
➢ "The Department of Homeland Security, properly supported by the Congress, should consolidate, as quickly as possible, a biometric entry-exit screening system, including a single system for spreading qualified travelers. It should be integrated with the system that provides benefits to foreigners seeking to stay in the United States. Linking biometric passports to good data systems and decisionmaking is a fundamental goal. No one can hide his or her debt by acquiring a credit card with a slightly different name. Yet today, a terrorist can defeat the link to electronic records by tossing away an old passport and slightly altering the name in the new one." (Ch. 12, p. 389)	➢ *DHS has established the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, an integrated, automated entry-exit system that records the arrival and departure of aliens; checks aliens' identities; and authenticates aliens' travel documents that are biometrically enabled. Already on line at 115 airports and 14 seaports for those travelers requiring a visa, US-VISIT will be extended by September 30 of this year to travelers from countries that participate in the Visa Waiver program, and then to all land ports of entry by December 31, 2005. Since January 2004, this new program has processed more than six million travelers and yielded nearly 800 matches to persons who were the subject of look-out bulletins.* ➢ *In terms of speeding "qualified travelers" through the system, the Transportation Security Administration (TSA) is testing the Registered Traveler Program (RTP) that allows aviation travelers in select domestic markets to provide TSA with certain biographical information and a biometric imprint (fingerprints and iris-scan). After passing a security assessment, RTP participants may use a dedicated lane at the airport for expedited screening.*

9

> "The U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation." (Ch. 12, p. 390)	> *Homeland Security Presidential Directive 6 (HSPD-6), issued on September 16, 2003, assigns a high priority to sharing terrorism-related information between and among responsible governments. The Department of State has been coordinating the overall effort to share with foreign governments the key watchlist and other information that could prove useful in identifying and apprehending terrorists. As one example, we now share our data on lost and stolen U.S. passports with other countries through INTERPOL. We have also committed, with our G-8 partners, to broader international information exchange through the Secure and Facilitated International Travel Initiative (SAFTI).*
> "Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists." (Ch. 12, p. 390)	> *Secure identification is a priority for the United States. Currently underway are several government initiatives enabling the Federal Government to better authenticate the identities of individuals seeking access to federally controlled facilities. For example, the Federal Identity Credentialing Committee, chartered by the Office of Management and Budget (OMB), is developing a common approach to identity badges and credentials across the Federal Government for employees and contractors. US-VISIT combats fraud in the travel documents of foreign nationals by obtaining biometric identifiers.* > *The President's senior advisors are also currently preparing recommendations on what additional steps can be taken in this area.*

➢ "Hard choices must be made in allocating limited resources. The U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort. The plan should assign roles and missions to the relevant authorities (federal, state, regional, and local) and to private stakeholders. In measuring effectiveness, perfection is unattainable. But terrorists should perceive that potential targets are defended. They may be deterred by a significant chance of failure." (Ch. 12, p. 391)	➢ *Homeland Security Presidential Directive 7 (HSPD-7), issued December 17, 2003, establishes "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." This effort includes development of the National Infrastructure Protection Plan. The Transportation Security Administration (TSA) is responsible for leading an interagency evaluation of the various modes of transportation to identify security gaps and response strategies.* ➢ *Other DHS actions taken include: (1) issuing Security Directives requiring protective measures to be implemented by passenger rail operators, and screening high-risk rail cargo entering the United States; (2) establishing the Highway Information Sharing and Analysis Center to link workers in the truck and bus industry to intelligence community analysts who collate, disseminate, and analyze threat information; (3) providing security grants and partnering with industry through various education and outreach efforts to improve bus, truck, and rail security; and (4) launching the Homeland Security Information Network (HSIN) that provides for real-time information to be shared between the DHS Homeland Security Operations Center (HSOC) and State and local agencies in responding to transportation-related or other terrorist incidents.* ➢ *Additionally, DHS and DOT are working with other Federal departments and agencies to evaluate potential long-term and short-term measures to protect rail shipments of hazardous materials, like chlorine, from deliberate attack.*
➢ "Improved use of 'no-fly' and 'automatic selectee' lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by the TSA, and it should utilize the larger set of watchlists maintained by the federal government. Air carriers should be required to supply the information needed to test and implement this new system." (Ch. 12, p. 393)	➢ *Expansion of the current "no-fly" and "selectee" lists is already underway as integration and consolidation of various watchlists by the Terrorist Threat Integration Center (TTIC) and the Terrorist Screening Center (TSC) progresses. International flight pre-screening is the responsibility of the new National Targeting Center (NTC) and domestic pre-screening the responsibility of Transportation Security Administration (TSA). The Administration is developing the next-generation approach to aviation passenger prescreening, implementation of which will enable the U.S. government to further expand the use of "no fly" and "selectee" lists to screen airline passengers in advance of their arrival at airports.*

"The TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. As a start, each individual selected for special screening should be screened for explosives. Further, the TSA should conduct a human factors study, a method often used in the private sector, to understand problems in screener performance and set attainable objectives for individual screeners and for the checkpoints where screening takes place." (Ch. 12, p. 393)	*The Transportation Security Administration (TSA) has made progress in improving the number and capability of the explosives detectors in place at our airports and our related procedures. For example, the National Explosives Detection Canine Team Program now oversees over 300 dog teams that provide coverage at each of the Nation's major airports. Outside the aviation context, in May 2004, TSA launched a test program to measure the feasibility of explosives screening for people and bags traveling on U.S. trains. In addition, several screening and other security technologies are under development, including an explosives detection portal for passengers to determine if explosives are being carried on an individual's person, document scanners to detect trace amounts of explosive materials on items such as boarding passes, and scanners for better screening of nasal and prosthetic devices.*
"As the President determines the guidelines for information sharing among government agencies and by those agencies with the private sector, he should safeguard the privacy of individuals about whom information is shared." (Ch. 12, p. 394)	*Throughout the development of the Terrorist Threat Integration Center (TTIC), the Terrorist Screening Center (TSC), and other information-sharing entities, new procedures and systems have been engineered with all applicable privacy and security issues in mind. The safeguarding of individual privacy is a key concern in the new rules DHS is presently developing on the protection of information specifically related to homeland security.*
"The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use." (Ch. 12, pp. 394-395)	*The Administration shares the Commission's dedication to preserving the constitutional freedoms that are the bedrock of our system of governance, and indeed, the Administration works every day to safeguard those freedoms. In addition, both Congress and the courts exercise substantial authority to oversee the executive branch's use of tools necessary to make America safer.* *In his most recent report to Congress on abuses concerning civil rights or civil liberties, the Inspector General of the Department of Justice advised that, of 162 complaints received alleging DOJ misconduct, "None ... related to their use of a substantive provision in the Patriot Act." (IG Report of January 27, 2004)*

➢ "At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties." (Ch. 12, p. 395)	➢ *The President issued a ban on the use of racial profiling by federal law enforcement, the first ever to do so.* ➢ *The Administration's commitment to these principles is demonstrated in part by the appointment of an Officer for Civil Rights and Civil Liberties and a Privacy Officer within the senior leadership of the Department of Homeland Security.* ➢ *In June the DHS Officer for Civil Rights & Civil Liberties submitted a report to Congress detailing DHS's successful efforts to carry out the President's commitment to the protection of civil liberties.* ➢ *DHS has taken strong steps to ensure that aliens detained in connection with a national security investigation will be provided timely notice of the charges against them, access to counsel, satisfactory detention conditions, an individualized review of the possibility of bond, and an individualized consideration for whether the immigration hearings should be closed or open to the public.* ➢ *The Justice Department's successful leadership in these efforts is also reflected in the section above.*
➢ "Homeland security assistance should be based strictly on an assessment of risks and vulnerabilities. Now, in 2004, Washington, D.C., and New York City are certainly at the top of any such list. We understand the contention that every state and city needs to have some minimum infrastructure for emergency response. But Federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support. Congress should not use this money as a pork barrel." (Ch. 12, p. 396)	➢ *As a result of historic funding increases sought by the President since 9/11, the Administration has allocated more than $13 billion to improve the terrorism preparedness of state and local first responders and public health agencies. The FY 2005 Budget request for these programs is 1400 percent above their FY 2001 funding level, and includes proposals to better target funds towards risks and vulnerabilities, such as doubling the Urban Area Security Initiative for "high-threat urban areas" to $1.4 billion. As the Administration agrees that such assistance should not be "revenue-sharing," Presidential homeland security directives require Federal departments and agencies providing preparedness assistance to first responders to base allocations on terror threat assessments, population concentrations, critical infrastructure, and similar risk factors, to the extent permitted by law. The Administration is developing nationwide risk-based preparedness goals which will help to further refine grant allocations.*

"Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven and effective frameworks for emergency response. We strongly support the decision that federal homeland security funding will be contingent, as of October 1, 2004, upon the adoption and regular use of ICS and unified command procedures. In the future, the Department of Homeland Security should consider making funding contingent on aggressive and realistic training in accordance with ICS and unified command procedures." (Ch. 12, p. 397)	*Homeland Security Presidential Directive 5 (HSPD-5), issued by the President on February 28, 2003, directs all Federal departments and agencies, beginning in FY 2005, to adopt the National Incident Management System (NIMS), and make its adoption a requirement for providing Federal preparedness assistance through grants, contracts, or other activities. The NIMS, which includes the Incident Command System (ICS) and a unified command structure, provides a consistent nationwide approach for Federal, state, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. A NIMS Integration Center, involving Federal, state, and local government representation, continues development and improvement of this system. DHS plans to conduct research in FY05 to develop location devices for first responders, and allow Incident Commanders to better understand where their resources are and how they are employed; and to provide virtual reality simulation training. The National Response Plan, to be completed in 2004, applies the incident command concepts to include Federal support to states and local governments during disasters. It will integrate operations into a seamless system and get help to victims more quickly and efficiently.*
"Congress should support pending legislation which provides for expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress." (Ch. 12, p. 397)	*The Department of Homeland Security is launching a new office that will coordinate federal, state, and local communications interoperability, leveraging both ongoing and new efforts to improve the compatibility of equipment, training, and procedures. As part of the RapidCom program, DHS is working with the state and local leadership in New York City, the DC Region, and eight other major cities to ensure that first responders can communicate by voice, regardless of frequency or mode during an emergency. In addition to these targeted efforts, interoperable communications planning and equipment has been a high priority for Federal homeland security assistance to states and localities, particularly in high-risk urban areas.*

A	"We endorse the American National Standards Institute's recommended standard for private preparedness. We were encouraged by Secretary Tom Ridge's praise of the standard, and urge the Department of Homeland Security to promote its adoption. We also encourage the insurance and credit-rating industries to look closely at a company's compliance with the ANSI standard in assessing its insurability and creditworthiness. We believe that compliance with the standard should define the standard of care owed by a company to its employees and the public for legal purposes. Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security." (Ch. 12, p. 398)	A	*Private-sector preparedness is a critical part of national preparedness. The Administration endorses the need for a standard of care for the duties and responsibilities of a company to its employees and the public. The Administration also believes in the importance of educating the public, on a continuing basis, about how to be prepared in case of a national emergency -- including a possible terrorist attack. To address this goal, the Department of Homeland Security has implemented the Ready Campaign, which is a national public service advertising campaign designed to educate and empower citizens to prepare for and respond to potential terrorist attacks and other emergencies. DHS will strengthen the success of the Ready Campaign by launching Ready for Business, a campaign specifically targeted to preparing businesses in the case of an emergency or terrorist attack. The Ready for Business Campaign is consistent with the recommendations contained within the ANSI standard.*

Chapter 13 "How to do it? A Different Way of Organizing the Government"	ACTIONS ALREADY TAKEN
➢ "We recommend the establishment of a National Counterterrorism Center (NCTC), built on the foundation of the Terrorist Threat Integration Center (TTIC). Breaking the older mold of national government organization, this NCTC should be a center for joint operational planning and joint intelligence, staffed by personnel from the various agencies. The head of the NCTC should have the authority to evaluate the performance of the people assigned to the Center." (Ch. 13, p. 403)	➢ *The President directed the establishment of the Terrorist Threat Integration Center (TTIC) in his 2003 State of the Union address, and TTIC began operations on May 1, 2003. The creation of the Terrorist Screening Center (TSC) was announced on September 16, 2003. These programs are significant steps taken in the direction of the recommended NCTC, as are the numerous forums for coordinated operational planning currently in use in the U.S. government.* ➢ *The President's senior advisors are currently preparing recommendations on how best to move forward in this area.*
➢ "The current position of Director of Central Intelligence should be replaced by a National Intelligence Director with two main areas of responsibility: (1) to oversee national intelligence centers on specific subjects of interest across the U.S. government and (2) to manage the national intelligence program and oversee the agencies that contribute to it." (Ch. 13, p. 411)	➢ *The President has laid out three principles for intelligence reform: (1) increasing the quality and quantity of human intelligence; (2) strengthening our technological capabilities to stay ahead of the terrorists; and (3) ensuring the most effective and coordinated use of these resources and personnel, because there are multiple agencies with intelligence responsibilities.* ➢ *The President's senior advisors are currently preparing recommendations on how best to move forward in this area.*
➢ "The CIA Director should emphasize (a) rebuilding the CIA's analytic capabilities; (b) transforming the clandestine service by building its human intelligence capabilities; (c) developing a stronger language program, with high standards and sufficient financial incentives; (d) renewing emphasis on recruiting diversity among operations officers so they can blend more easily in foreign cities; (e) ensuring a seamless relationship between human source collection and signals collection at the operational level; and (f) stressing a better balance between unilateral and liaison operations." (Ch. 13, p. 415)	➢ *CIA initiated new efforts to expand its collection and analytical capabilities even before 9/11. CIA's efforts were greatly accelerated in the wake of the attacks, including through hiring, training, and deploying a cadre of new highly-qualified human source collectors and analysts at an unprecedented rate, the implementation of a new language program, integration of human and electronic intelligence, and increased focus on unilateral (non-liaison) sources.* ➢ *The CIA has a sophisticated metrics program allowing senior Agency managers to measure progress against its goals. The CIA Executive Board meets at least bi-monthly to review each metric, make adjustments in plans where necessary, and reaffirm priorities.* ➢ *The President's senior advisors are currently preparing recommendations on how best to ensure continued progress in this area.*

▲ "Lead responsibility for directing and executing paramilitary operations, whether clandestine or covert, should shift to the Defense Department. There it should be consolidated with the capabilities for training, direction, and execution of such operations already being developed in the Special Operations Command." (Ch. 13, p. 415)	▲ *CIA paramilitary officers and DoD officers have performed together exceptionally in the field, including in both Afghanistan and Iraq. Close coordination and joint planning between CIA and military special operators is standard.* ▲ *The President's senior advisors are currently preparing recommendations on what steps can be taken to ensure continued optimal CIA/DOD coordination in the future.*
▲ "Finally, to combat the secrecy and complexity we have described, the overall amounts of money being appropriated for national intelligence and to its component agencies should no longer be kept secret. Congress should pass a separate appropriations act for intelligence, defending the broad allocation of how these tens of billions of dollars have been assigned among the varieties of intelligence work." (Ch. 13, p. 416)	▲ *The overall intelligence Community appropriation has been declassified twice in recent years (in fiscal years 1997 and 1998), when a specific determination was made that the figure for that year could be released safely.* ▲ *The President's senior advisors are currently preparing recommendations on what steps can be taken in this area consistent with national security requirements.*

➢ "Information procedures should provide incentives for sharing, to restore a better balance between security and shared knowledge." (Ch. 13, p. 417)	➢ *The President established the Terrorist Threat Integration Center (TTIC), integrating and analyzing terrorism threat-related information collected domestically and abroad, ensuring that intelligence and law enforcement entities are working in common purpose.* ➢ *The Terrorist Screening Center (TSC) was established to consolidate terrorist watchlists and provide 24/7 operational support for thousands of Federal screeners across the country and around the world. The Center ensures that government investigators, screeners, and agents are working with the same unified, comprehensive set of anti-terrorist information – and that they have access to information and expertise that will allow them to act quickly when a suspected terrorist is screened or stopped.* ➢ *With the development of the Terrorist Threat Integration Center (TTIC) and the Terrorist Screening Center (TSC) has come a series of steps, including agreement, on March 4, 2003, by key federal departments and agencies, to a comprehensive Memorandum of Understanding to break down barriers to information sharing, increase the writing of intelligence products with unclassified "tear-line" versions, reduce information controls to the extent consistent with our national security, and take other steps in this direction.* ➢ *Since 9/11, the FBI has continued to enhance its longstanding practice of sharing terrorism threat-related information with state and local law enforcement through its joint terrorism task forces.* ➢ *The Administration is also developing guidelines and regulations to improve information-sharing both among Federal Departments and Agencies and between the Federal Government and state and local entities.* ➢ *The President's senior advisors are currently preparing recommendations on how best to ensure continued progress in this area.*

18

➢ "The president should lead the government-wide effort to bring the major national security institutions into the information revolution. He should coordinate the resolution of the legal, policy, and technical issues across agencies to create a 'trusted information network.'" (Ch. 13, p. 418)	➢ *Since 2001, the President has improved intelligence collection, analysis, and sharing to obtain the best picture of the terrorist threat to the Nation. An important part of each of the major organizational changes since 9/11 has been conscious attempts to increase database accessibility to those who need information, while, at the same time, building into our information-sharing architecture safeguards both for security and privacy. Information technology advances in these areas have been integral parts of the development of the TTIC, TSC, and other efforts, including the following:* o *DHS launched the Homeland Security Information Network (HSIN), a real-time collaboration system used by more than one thousand first responders, mainly from the law enforcement community, to report incidents, crimes and potential terrorist acts to one another and the DHS Homeland Security Operations Center.* o *The Department of Defense created U.S. Northern Command, to provide for integrated homeland defense and coordinated DoD support for Federal, state, and local civilian governments.* o *President Bush signed the USA PATRIOT Act, which strengthens law enforcement's abilities to prevent, investigate, and prosecute acts of terror, facilitating Federal government efforts to thwart potential terrorist activity throughout the United States. The President continues to call on Congress to take action to ensure that these vital law enforcement tools do not expire.* ➢ *The President's senior advisors are currently preparing recommendations on how best to ensure continued progress in this area.*

• "Since a catastrophic attack could occur with little or no notice, we should minimize as much as possible the disruption of national security policymaking during the change of administrations by accelerating the process for national security appointments. We think the process could be improved significantly so transitions can work more effectively and allow new officials to assume their responsibilities as quickly as possible." (Ch. 13, p. 422)	• *The Administration agrees that minimizing disruption to the national security policymaking process is critical, including expediting the process for national security appointments.* • *The Administration supports the Commission's view that the Senate should take steps to speed confirmations at the beginning of an administration and its recommendation that the number of positions requiring Senate confirmation should be reduced.* • *In addition, the Federal government has in place robust programs to ensure that essential functions of government, such as uninterrupted continuity of leadership and policymaking mechanisms, continue during emergencies. We continue to work to improve the effectiveness of these continuity programs to minimize disruption of critical governmental functions.* • *As noted by the 9/11 Commission, responsibility for improving transitions lies largely with Presidents-elect and with Congress. The President's senior advisors are currently preparing recommendations on what the Executive Branch can do to move forward in this area.*
• "A specialized and integrated national security workforce should be established at the FBI consisting of agents, analysts, linguists, and surveillance specialists who are recruited, trained, rewarded, and retained to ensure the development of an institutional culture imbued with a deep expertise in intelligence and national security." (Ch. 13, pp. 425-426)	• *The FBI has implemented a strategic plan to recruit, hire, and retain Intelligence Analysts. The Bureau has selected veteran analysts to attend events at colleges, universities, and designated career fairs throughout the country. It executed an aggressive public recruiting plan and, for the first time in FBI history, is offering hiring bonuses for FBI analysts. In its Special Agent hiring, the FBI has changed the list of "critical skills" it is seeking in candidates to include intelligence experience and expertise, foreign languages, and technology.* • *The FBI continues to grow the Field Intelligence Groups (FIGs) established in every FBI field office and is on track to add some 300 Intelligence Analysts to the FIGs in FY 2004. The FIGs conduct analysis, direct the collection of information to fill identified intelligence gaps, and ensure that information is disseminated horizontally and vertically to internal and external customers, including our state, local and tribal partners. As of June 2, 2004, there are 1,450 FIG personnel, including 382 Special Agents and 169 employees from other government agencies. To support information sharing, there is now a Special Agent or Intelligence Analyst in each Joint Terrorism Task Force (JTTF) dedicated to producing "raw" intelligence reports for the entire national security community, including, as appropriate, state, municipal, and tribal law enforcement partners and other JTTF members. These "Reports Officers" are trained to produce intelligence reports that both maximize the amount of information shared and, equally important, protect intelligence or law enforcement sources and methods and privacy interests.* • *The President's senior advisors are currently preparing recommendations on how best to ensure continued progress in this area.*

▲ "The Department of Defense and its oversight committees should regularly assess the adequacy of Northern Command's strategies and planning to defend the United States against military threats to the homeland." (Ch. 13, p. 428)	▲ *The Department of Defense created U.S. Northern Command (NORTHCOM), and principal responsibility for defending the homeland is now assigned to a four-star unified military commander wielding capabilities and resources that did not exist prior to 9/11.* ▲ *The Secretary of Defense already provides significant oversight of NORTHCOM, as do numerous Congressional committees.* ▲ *The President's senior advisors are currently preparing recommendation on what additional steps, if any, may be needed to ensure the defense of the United States against threats to the homeland.*
▲ "The Department of Homeland Security and its oversight committees should regularly assess the types of threats the country faces to determine (a) the adequacy of the government's plans—and the progress against those plans—to protect America's critical infrastructure and (b) the readiness of the government to respond to the threats that the United States might face." (Ch. 13, p. 428)	▲ *Homeland Security Presidential Directive 7 (HSPD-7) details the roles and responsibilities of the Department of Homeland Security (DHS) and other Federal departments and agencies in protecting national critical infrastructure. DHS is currently working with all Federal departments and agencies to develop a comprehensive, cross-sector National Critical Infrastructure Protection Plan. The plan will be completed by this fall and will be reviewed annually for its adequacy in protecting against current threats. Additionally, with the creation in March 2003 of the Information Analysis and Infrastructure Protection (IAIP) directorate within DHS, the United States now has a single focal point for the matching of real-time threat information with potential vulnerabilities in national critical infrastructure. Furthermore, Homeland Security Presidential Directive 8 (HSPD-8) directs the development of a measurable National Preparedness goal and a training and exercise program to ensure that the Federal Government, states, and localities are making progress toward that goal.* ▲ *The President's senior advisors are currently preparing recommendations on what additional steps might be taken to ensure the protection of America's critical infrastructure.*

JOHN CORNYN

United States Senator - Texas
CONTACT: DON STEWART
(202) 224-0704 office
(202) 365-6702 cell
don_stewart@cornyn.senate.gov

FOR IMMEDIATE RELEASE
August 19, 2004

9/11 COMMISSIONERS URGE FOCUS ON BORDER SECURITY

Cornyn says testimony highlights need for immigration reform

WASHINGTON--In testimony before the Senate Judiciary Committee Thursday, Commissioners Lee Hamilton and Slade Gorton of the 9/11 Commission highlighted the importance of "a unified program to speed known travelers, so inspectors can focus on those travelers who might present greater risks. This is especially important for border communities." U.S. Sen. John Cornyn, a member of the committee's Immigration, Border Security and Citizenship subcommittee, said the commissioners' remarks highlight the need for immigration reform.

"As we implement the recommendations of the 9/11 Commission, we must recognize that border security and immigration reform go hand in hand. Our immigration system needs to distinguish between the benign and the dangerous, and our law enforcement resources must be dedicated to hunting potential terrorists and other threats to our homeland. This requires a true reform of our immigration system, and a fresh look at our law enforcement priorities," Cornyn said. "It's critical that we focus our efforts on finding and removing criminals, and preventing those who would do us harm from entering in the first place."

In an effort to reform immigration policy and re-center law enforcement on border security, Cornyn introduced the *Border Security and Immigration Reform Act* (S. 1387) in July, 2003. The legislation is a comprehensive immigration reform to develop a temporary worker program and strengthen homeland security efforts at the borders. Identifying those who are here to work and then return home would allow law enforcement to focus on those who attempt to enter the United States illegally, or worse, enter for purposes of committing terrorist acts.

"We must continue to ensure that those who follow the law will benefit from easier travel, while making clear that those who fail to comply with our immigration and other laws will face severe and immediate consequences," Cornyn said.

Sen. Cornyn chairs the subcommittee on the Constitution, Civil Rights & Property Rights. He is the only former judge on the Judiciary Committee and served previously as Texas Attorney General, Texas Supreme Court Justice, and Bexar County District Judge.

30

http://cornyn.senate.gov

News From:
U.S. Senator
Russ Feingold

506 Hart Senate Office Building
Washington, D.C. 20510-4904
(202) 224-5323

http://www.senate.gov/~feingold

Contact: **Trevor Miller**
(202) 224-8657

Statement of U.S. Senator Russ Feingold
At the Senate Judiciary Committee Hearing on "The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security"

August 19, 2004

Thank you, Mr. Chairman, for holding this hearing. I also want to thank Commissioners Hamilton and Gorton and all the members and staff of the 9/11 Commission for your incredibly important and effective service. I can't emphasize enough how vital your work is to the American people, and how significant and refreshing it is that your report and recommendations are bipartisan and unanimous.

I supported the creation of the 9/11 Commission because I believed it was crucial to review what went wrong leading up to that fateful day in September three years ago, what we can learn from those mistakes, and what we should do to improve our nation's defenses against a future attack. But I will confess that the product greatly exceeded my expectations, and even my hopes. You have provided us with a template for how to make the country safer and stronger.

It is now time to implement these recommendations. We need to work out the details carefully but quickly and in a bipartisan manner, taking our cue from the work of the Commission. Our nation must effectively combat the terrorist threat we face. That must be the very highest priority of the Congress. We need real reforms now, particularly with regard to our intelligence community and intelligence oversight. I look forward to working with my colleagues, on both sides of the aisle to make the bipartisan recommendations of the Commission a reality.

###

1600 Aspen Commons
Middleton,WI 53562
(608) 828-1200

517 E. Wisconsin Ave.
Milwaukee, WI 53202
(414) 276-7282

First Star Plaza
401 5th St., Room 410
Wausau, WI 54403
(715) 848-5660

425 State St., Room 232
La Crosse, WI 54603
(608) 782-5585

1640 Main Street
Green Bay, WI 54302
(920) 465-7508

Testimony to the Senate Judiciary Committee meeting on the 9-11 Commission Recommendations
Thursday, August 19th

Mr. Chairman, members of the Committee: Families of September 11 would like to thank you for holding these hearings and for the opportunity to have a statement read into testimony today. We are a group of families whose loved ones were killed on September 11 and whose organization now represents more than 2000 families and survivors.

In the months following September 11, 2001, the families began to advocate for the creation of a commission to investigate the terrorist attacks with the goal of making whatever changes would be necessary to prevent another such attack. The result of the work of the 9-11 Commission – a report that is a bestseller by anyone's calculation – illustrates beyond doubt that fundamental organizational reforms must be undertaken if the government is to create an intelligence community worthy of the name, worthy of the trust of the American people and worthy of the sacrifice involved in the work of the intelligence officers who labor to serve the nation

The American people are reading this report closely. They are absorbing the recommendations. They are watching what you do here today and what you will do in the weeks and months ahead. Not only the 9-11 families but the public at large will not be pleased if they see the Commission's recommendations falling by the wayside.

Certainly these hearings are an important beginning and we appreciate that the members of this committee have interrupted their recesses to address the most serious issue facing all Americans. However, the encouragement that the families and our country receive from the timeliness of these hearings is tempered by a very real fear: that Congress and the Administration will not act expeditiously. It is crucial that the implementation of the Commission's recommendations occur on a timeline that is drawn to protect America, not to protect existing public servants or incumbents of any party.

Yes, it is vital for our nation that we avoid quick fixes that are inadequate or incomplete. At the same time, subjecting these recommendations to endless debate, whether out of political posturing or bureaucratic entrenchment, is intolerable.

Therefore, we ask that you consider the following:

First, recognize that the unprecedented terrorist attacks of September 11 demand an unprecedented Congressional effort to streamline the committee process, coordination between the legislative and executive branches of the government and recognition of the vital role played by the judiciary in the tripartite balance of power established in our Constitution. Although tensions among these branches of government are essential, they cannot be allowed to produce paralysis.

Second, provide the American people with a timetable that Congress is prepared to follow to implement this report. Legislation that is enacted in response to these recommendations must not be allowed to gather dust until another tragedy forces Congress to respond with remedial legislation

Lastly, keep the Commission alive to oversee the implementation of its recommendations. This bipartisan body is uniquely qualified to inform you, your colleagues and the broader public as

debate sharpens our focus on necessary change, monitor implementation of those changes and reassure the American people that the process is working – that the progress being made by our elected leaders is furthering our security while assuring our basic freedoms, and that all of the recommendations are properly implemented.

The 9/11 families have endorsed the Commission's recommendations as a whole. We hope that you recognize that they are **all** important and are **all** part of a comprehensive package designed to work in concert to significantly diminish the terrorist threat facing our country.

The Commission report deals with issues that go beyond intelligence czars and counter terrorism centers – issues that have led the news in recent days. The Commission has made important recommendations that deal with issues of foreign policy, border security, terrorist financing, economic policy and the like. We implore you to prioritize, to enact that which can be carried out **immediately**, while also moving forward on recommendations requiring longer-term discussion.

We are looking to you and your colleagues to do your work quickly and to do it right. These are not incompatible goals. Now is your opportunity. Implement these recommendations and demonstrate to the American public that you are serious in your efforts.

Mr. Chairman, please do what is required. Act wisely and quickly. The families look forward to working closely with you and the rest of the committee to do what is necessary.

Today is the now, the here, through which all future plunges to the past. Please help us make that past less painful for others than it was for those we loved and lost.

Sincerely,

Donald Goodrich,
Chairman of the Board
Families of September 11
Father of Pete, killed 9-11-01

Prepared Statement of Vice Chair Lee Hamilton
and Commisioner Slade Gorton
National Commission on Terrorist Attacks Upon the United States
before the Senate Committee on the Judiciary
August 19, 2004

The 9/11 Commission Report

Chairman Hatch, Ranking Member Leahy, other distinguished Members of the Committee: We are honored by the opportunity to appear before you today. We are grateful to you, and to the Leadership of the Senate, for your prompt consideration of the Report and recommendations of the Commission.

As you know, the Commission's findings and recommendations were strongly endorsed by all Commissioners – five Republicans and five Democrats who have been active in the public life of our nation. In these difficult times, and in an election year, we think this unanimity is remarkable, and important. It reflects a unity of purpose to make our country safer and more secure in the face of the novel threat posed by transnational terrorism. We call upon the Congress and the Administration to respond to our Report in the same spirit of bipartisanship.

You have asked us discuss three subjects of special interest to this Committee: our findings and recommendations with respect to the Federal Bureau of Investigation; border security; and the USA PATRIOT Act. We will discuss each of these areas in turn.

The FBI

The FBI has for the past several decades performed two important but related functions. First, it serves as our premier federal law enforcement agency, investigating possible violations of federal criminal statutes and working with federal prosecutors to develop and bring cases against violators of those laws. Second, it is an important member of the Intelligence Community, collecting information on foreign intelligence or terrorist activities within the United States. That information can be used either for additional counterintelligence or counterterrorism investigation or to bring criminal prosecutions.

We focused on the FBI's performance as an intelligence agency combating the al Qaeda threat within the United States before 9/11. Like the Joint Inquiry of the Senate and House Intelligence Committees before us, we found that performance seriously deficient. Director Freeh did made counterterrorism a priority in the 1990s, and Dale Watson, his Counterterrorism chief, made valiant efforts to communicate that priority to agents in the field. But that priority did not effectively find its way into the daily work of the FBI's field offices. Nor did it result in the creation of a corps of intelligence officers and analysts with the professional qualifications and skills needed for an effective intelligence/counterterrorism operation.

Finally, when FBI agents did develop important information about possible terrorist-related activities, that information often did not get effectively communicated – either within the FBI itself or in the Intelligence Community as a whole.

Within the FBI itself, communication of important information was hampered by the traditional case-oriented approach of the agency and the possessive case-file mentality of FBI agents. And this Committee is only too familiar with the information technology problems that have long hampered the FBI's ability to "know what it knows." Even when information was communicated from the field to headquarters, it did not always come to the attention of the Director or other top officials who should have seen it. This was the case in the now-famous incidents, in the summer of 2001, of the Phoenix electronic communication about Middle Eastern immigrants in flight schools, and the Minneapolis Field Office's report to headquarters about the arrest of Zacarias Moussaoui.

The other internal barrier to communication of intelligence information between FBI intelligence officials and FBI criminal agents and federal prosecutors was the "wall" between intelligence and law enforcement that developed in the 1980s and was reinforced in the 1990s. Through a combination of court decisions, pronouncements from the Department of Justice and its Office of Intelligence Policy and Review, and risk-averse interpretations of those pronouncements by the FBI, the flow of information between the intelligence and criminal sides of the FBI and the Justice Department was significantly choked off – a phenomenon that continued until after 9/11, when the Congress enacted the USA PATRIOT Act, and when the Justice Department successfully appealed a FISA Court decision that had effectively reinstated the wall.

These failures in internal communications were exacerbated by a reluctance of the FBI to share information with its sister agencies in the Intelligence Community, with the National Security Council at the White House, and with state and local law enforcement agencies. This culture of non-sharing was by no means unique to the FBI, but the FBI was surely one of the worst offenders.

The FBI, under the leadership of its current Director, Robert Mueller, has undertaken significant reforms to try to deal with these deficiencies and build a strong capability in intelligence and counterterrorism. These include the establishment of an Office of Intelligence, headed by an Associate Director, Maureen Baginski, who is an experienced manager of intelligence systems. The FBI has embarked on an ambitious program to recruit qualified analysts, to train all agents in counterterrorism, and to develop career tracks for agents who want to specialize in counterterrorism or intelligence. The agency is also making progress, albeit slowly, in upgrading its internal information technology system. But, as Director Mueller himself has recognized, much more remains to be done before the FBI reaches its full potential as an intelligence agency.

Because of the history of serious deficiencies, and because of lingering doubts about whether the FBI can overcome its deep-seated law-enforcement culture, the Commission gave serious consideration to proposals to move the FBI's intelligence operations to a

new agency devoted exclusively to intelligence collection inside the United States – a variant of the British Security Service, popularly known as MI-5.

We decided not to make such a recommendation for several reasons, set forth in our Report. Chief among them were the disadvantages of separating domestic intelligence from law enforcement and losing the collection resources of FBI field offices around the country, supplemented by relationship with state and local law enforcement agencies. Another major reason was civil liberties concerns that would arise from creating outside the Justice Department an agency whose focus is on collecting information from and about American citizens, residents, and visitors. The rights and liberties of Americans will be better safeguarded, we believe, if this sensitive function remains in an agency trained and experienced in following the law and the Constitution, and subject to the supervision of the Attorney General.

We also believe that while the jury is still out on the ultimate success of the reforms initiated by Director Mueller, the process he has started is a promising one. And many of the benefits that might be realized by creating a new agency will be achieved, we are convinced, if our important recommendations on restructuring of the Intelligence Community – creation of a National Counterterrorism Center and a National Intelligence Director with real authority to coordinate and direct the activities of our intelligence agencies – are implemented. An FBI that is an integral part of the NCTC and is responsive to the leadership of the National Intelligence Director will work even more effectively with the CIA and other intelligence agencies, while retaining the law enforcement tools that continue to be an essential weapon in combating terrorism.

What the Commission recommends, therefore, is that further steps be taken – by the President, the Justice Department, and the FBI itself -- to build on the reforms that have been undertaken already, and to institutionalize those reforms so that the FBI is transformed into an effective intelligence and counterterrorism agency. The goal, as our Report states, is to create within the FBI a specialized and integrated national security workforce of agents, analysts, linguists, and surveillance specialists who create a new FBI culture of expertise in national security and intelligence. This Committee will have a vital oversight role in monitoring progress by the FBI and ensuring that this new capacity so critical to our nation is created and maintained.

Border Control

As our Report makes clear, in the decade before 9/11, border security was not seen as a national security matter. From a strategic perspective, border policy focused on counternarcotics efforts, illegal immigration, and, more recently, the smuggling of weapons of mass destruction. Our government simply did not exhibit a comparable level of concern about terrorists' ability to enter and stay in the United States.

During that same period, however, al Qaeda studied how to exploit gaps and weaknesses in the passport, visa, and entry systems of the United States and other countries. Al Qaeda actually set up its own passport office in Kandahar and developed working

relationships with travel facilitators – travel agents (witting or unwitting), document forgers, and corrupt government officials.

As we know, Al Qaeda's travel tactics allowed the 9/11 hijackers to enter the United States quite easily. Yet the Commission found that many of the 19 hijackers were potentially vulnerable to detection by border authorities. Although the intelligence as to their tactics was not developed at the time, examining their passports could have allowed authorities to detect from four to 15 hijackers. More effective use of information in government databases could have allowed border authorities to intercept up to three of the hijackers had they been watchlisted.

More robust enforcement of routine immigration laws, supported by better information, could also have made a difference. Two hijackers made statements on their visa applications that could have been shown to be false by U.S. government records available to consular officers. Many of the hijackers lied about their employment or educational status. Two hijackers could have been denied admission at the port of entry based on violations of immigration rules governing terms of admission. Three hijackers violated the immigration laws after entry, one by failing to enroll in school as declared, and two by overstays of their terms of admission.

Neither the intelligence community, nor the border security agencies or the FBI, had programs in place to analyze and act upon intelligence about terrorist travel tactics – how they obtained passports, made travel arrangements, and subverted national laws and processes governing entry and stays in foreign countries.

Congress during the 1990s took some steps to provide better information to immigration officials by legislating requirements for a foreign student information system and an entry-exit system. As we know, these programs were not successfully implemented before 9/11.

Since 9/11, some important steps have been taken to strengthen our border security. The Department of Homeland Security has been established, combining the resources of the former Immigration and Naturalization Service and the Customs Bureau into new agencies to protect our borders and to enforce the immigration laws within the United States. The visa process and the terrorist watchlist system have been strengthened. DHS has begun to implement, through the US VISIT program, a biometric screening system for use at the border.

These efforts have made us safer, but not safe enough. As a nation we have not yet fully absorbed the lessons of 9/11 with respect to border security. The need to travel makes terrorists vulnerable. They must leave safe havens, travel clandestinely, and use evasive techniques, from altered travel documents to lies and cover stories. Terrorist entry often can be prevented and terrorist travel can be constrained by acting on this knowledge. Targeting terrorist travel is at least as powerful a weapon against terrorists as targeting their finances.

The Commission therefore has recommended that we combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility.

Targeting Terrorist Travel

Front line border agencies must not only obtain from the Intelligence Community – on a real-time basis information on terrorists; they must also assist in collecting it. Consular officers and immigration inspectors, after all, are the people who encounter travelers and their documents. Specialists must be developed and deployed in consulates and at the border to detect terrorists through their travel practices, including their documents. Technology has a vital role to play. The three years since 9/11 have been more than enough time for border officials to integrate into their operations terrorist travel indicators that have been developed by the intelligence community. The intelligence community and the border security community have not been close partners in the past. This must change.

We also need an operational program to target terrorist travel facilitators -- forgers, human smugglers, travel agencies, and corrupt border officials. Some may be found here, but most will be found abroad. Disrupting them would seriously constrain terrorist mobility. While there have been some successes in this area, intelligence far outstrips action. This should be rectified by providing the interagency mandate and the necessary resources to Homeland Security's enforcement arm, Immigration and Customs Enforcement (ICE), and other relevant agencies, including the FBI.

This problem illustrates the need for a National Counterterrorism Center. Investigations of travel facilitators raise complicated questions: Should a particular travel facilitator be arrested or should he be the subject of continued intelligence operations? In which country should he be arrested? The NCTC could bring the relevant intelligence agencies to the table to coordinate and plan the best course of action.

Screening Systems

To provide better information to our consular officers and immigration inspectors, the government must accelerate its efforts to build a biometric entry and exit screening system. This is an area in which Congress has been active since the mid-1990's. It has been a frustrating journey. Congress first legislated an entry-exit system in 1996, to increase compliance with our immigration laws. It was not associated with counterterrorism, nor with biometric identification. As a practical matter, the entry-exit effort was not seriously funded until the end of 2002. By that time, aspects of a system were governed by four separate laws. The establishment of the Department of Homeland Security then changed the organizational context for implementing those laws.

The new Department is emerging from its difficult start-up period and is, we believe, poised to move forward to implement Congress's mandates in this area. We would like to stress four principles that we believe must guide our efforts in this arena.

First, the U.S. border security system must be an effective part of a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The Department of Homeland Security should lead an effort to design a comprehensive screening system, addressing common problems and setting common standards with system-wide goals in mind.

Second, a biometric entry and exit screening system is fundamental to intercepting terrorists and its development should be accelerated. Each element of the system is important. The biometric identifier makes it difficult to defeat a watchlist by an alteration in spelling of a name, a technique relied upon by terrorists. The screening system enables border officials access to all relevant information about a traveler, in order to assess the risk they may pose. Exit information allows authorities to know if a suspect individual has left the country and to establish compliance with immigration laws.

Third, United States citizens should not be exempt from carrying biometric passports or otherwise enabling their identities to be securely verified. Nor should Canadians or Mexicans.

Fourth, there should be a unified program to speed known travelers, so inspectors can focus on those travelers who might present greater risks. This is especially important for border communities.

We believe that the schedule for completion of this biometric entry-exit screening system should be accelerated to the extent feasible. This will require additional annual funding, and a mandate to a central organizational authority, such as the US VISIT office, to manage the effort.

International Collaboration

We need to dedicate a much greater effort to collaboration with foreign governments with respect to border security. This means more exchange of information about terrorists and passports, and improved global passport design standards. Implicit in this recommendation is continued close cooperation with Mexico and Canada. One particularly important effort is to improve screening efforts prior to departure from foreign airports, especially in countries participating in the visa waiver program.

Immigration Law and Enforcement

We must be able to monitor and respond to entries along our long borders with Canada and Mexico, working with those countries as much as possible. Our law enforcement system ought to send a message of welcome, tolerance, and justice to members of the immigrant communities in the United States, while also fostering the respect for the rule of law. Good immigration services are one way to reach out that is valuable, including for intelligence. State and local law enforcement agencies need more training and

partnerships with federal agencies so they can cooperate more effectively with those federal authorities in identifying terrorist suspects.

Finally, secure identification should begin in the United States. We believe that the federal government should set standards for the issuance of birth certificates and sources of identification such as drivers' licenses.

The agenda on immigration and border control, then, is multi-faceted and vital to our national security. The bottom line is that our visa and border control systems must become an integral part of our counterterrorism intelligence system. We must steer a course that remains true to our commitment to an open society that welcomes legitimate immigrants and refugees while concentrating our resources on identification of potential of potential terrorists and prevention of their entry into the United States.

The USA PATRIOT Act

The USA PATRIOT Act, passed in the wake of the 9/11 attacks, was substantially the product of this Committee. A number of provisions of the Act were relatively noncontroversial, updating existing authorities to take account of the digital age. But others were more far-reaching – granting to the FBI, the Department of Justice and other Executive Branch agencies important new authorities to use in combating terrorism. For this reason, the Congress chose to sunset many of the provisions of the Act at the end of next year. We know that this Committee, and the House Committee on the Judiciary, will be holding hearings to determine whether to extend these expiring provisions and whether to make additional changes in the law.

The Commission did not canvass the entire range of issues raised by the USA PATRIOT Act in detail. We have limited our specific recommendations with respect to the USA PATRIOT Act to those provisions that bear most directly on our mandate – i.e., those that relate to information sharing in the intelligence and law enforcement communities. We believe that those provisions – breaking down the wall that prevented the FBI from sharing intelligence information gathered under the Foreign Intelligence Surveillance Act (FISA) with federal prosecutors, and allowing the Justice Department to share grand jury information with other intelligence and law enforcement agencies – should be extended. They are important in their own right, and they have helped spur the increased sharing of information throughout the Intelligence Community that is vital to a successful counterterrorism program.

We made a general recommendation that applies not only to consideration of other provisions of the USA PATRIOT Act, but also to other legislative or regulatory proposals that may impinge on individual rights or liberties, including personal privacy. The burden in all cases should be on those proposing the restriction to show that the gains that will flow in terms of national security are real and substantial, and that individual rights and liberties will be adequately protected. We recommend the establishment of appropriate guidelines for such programs. We also recommend the establishment in the

executive branch of an oversight office or board to be a watchdog to assure maximum protection of individual rights and liberties in these programs.

We conclude with what we said in our Report:

> We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.

We would be pleased to respond to your questions.

Statement of Sen. Orrin G. Hatch
before the
United States Senate Judiciary Committee
Hearing on

"THE 9/11 COMMISSION REPORT AND RECOMMENDATIONS FOR THE FUTURE OF FEDERAL LAW ENFORCEMENT AND BORDER SECURITY"

Let me begin by adding my voice to those who have expressed their appreciation of the members of the 9/11 Commission and their staff for their hard work in putting together a thorough report that includes many thoughtful recommendations.

Thank Senator Gorton and thank you Representative Hamilton.

We also owe a debt of gratitude to all of the witnesses who appeared before the Commission, especially the representatives of the families of those who perished in the horrific and unjustified attacks of nearly three years ago.

The first responsibility of government is to protect its citizens and we must never shy away from this duty.

Today the Judiciary Committee begins its discussion of the portions of the 9/11 Commission's Report and recommendations that relate to areas under our jurisdiction such as border security and the role of the FBI in the field of counterintelligence.

Our colleagues on the Government Affairs Committee, led by Senator Collins and Lieberman, have asked for our Committee's perspective on matters within our expertise and I thank them.

In addition to those recommendations that are designed to help our law enforcement and homeland security agencies identify, thwart, and apprehend terrorists, we on the Judiciary Committee have a special role in implementing and overseeing any recommendations aimed at protecting our civil liberties. I expect, for example, that today's hearing will help us gain a better understanding of the Commission's recommendation calling for the creation of a new civil liberties board.

Similarly, we must take to heart the Commission's recommendation with respect to our obligation to provide humane treatment for those detained as suspected or captured terrorists. The abuse of prisoners such as occurred at Abu Ghraib is contemptible as well as counterproductive to our efforts to stop Islamist terrorism at its countries of origin.

Much attention that been focused on the now-famous organizational chart on page 413 of the Commission Report proposing the National Intelligence Director, the National

Counterterrorism Center, and the three, dual-hatted deputies. As significant as the debate today over the structural issues is, it must not be allowed to crowd out an equally important public policy discussion of those recommendations that urge America to stand up for and defend our core values and ideals with our foreign neighbors and work to bring about long term changes in the underlying economic and political conditions that foster Islamist terrorism in certain regions.

We must not be under any illusion that we can reach accommodations with Islamist terrorist organizations like Al Qeada. The Commission found that these groups do not hold views "with which Americans can bargain or negotiate .... there is no common ground – not even respect for life -- on which to begin a dialogue... [They] can only be destroyed or utterly isolated."

The deadly attacks on 9/11 required our country to adopt new laws to protect the public. I find constructive the Commission's observation that "a full and informed debate on the Patriot Act would be healthy." In this regard, I would note that the Commission also found that, (s)ome executive actions that have been criticized are unrelated to the Patriot Act. The provisions that facilitate the sharing of information among intelligence agencies and between law enforcement and intelligence appear, on balance, to be beneficial."

The 9/11 Commission Report documents the negative repercussions of the so-called wall that existed before enactment of the Patriot Act between intelligence and criminal investigators. Even if the Commission is accurate in its assessment that the July 1995 procedures establishing the wall by Attorney General Reno "were almost immediately misunderstood and misapplied," there can be no doubt, as chapter eight of the Report lays out in great detail, that creation of the wall between intelligence and criminal investigators impeded rigorous following of leads that may have prevented the 9/11 attacks.

The Commission's Report catalogs that on August 29, 2001 one frustrated FBI criminal investigator prophetically e-mailed across the wall to a FBI intelligence officer the following message after being denied the ability to access and use information about one key Al Qeada operative:

> "... someday someone will die – and wall or not – the public will not understand why we were not more effective and throwing every resource we had at certain 'problems'."

Never were more truer words written. But our job is to learn from our past mistakes in order to protect the American public in the future.

If we carefully review the lessons contained in the 9/11 Commission Report and fairly evaluate its recommendations, we will be able to better marshal our resources and carry out our Counterterrorism program more effectively and reduce the risk of terrorist attacks against Americans at home and abroad.

For example, the Commission's Report compellingly demonstrates the importance of border security and tracking international travelers. Under Secretary Hutchinson will help us understand the Administration's views in this critical area.

Also of great interest to the Judiciary Committee is the Commission's recommendation relating to the future of the FBI in the war against terrorism. The 9/11 Commission Report found that the FBI and Director Mueller have cooperated with the Commission. Recently, the FBI issued its formal response to the Commission's recommendations and, in each instance, was either implementing it or reexamining its current policy in light of the recommendation.

I would like to commend President Bush for his leadership in making certain that the key senior Administration officials are giving the bi-partisan 9/11 Commission Report the respect and consideration it merits.

It appears to me that, by and large, all of the Committees in the House and Senate are attempting to approach the Report in a bipartisan manner despite the fact that we are deep into the election cycle and despite the fact that some of the Commission's recommendations are somewhat complex and controversial such as those pertaining to changes in Congressional oversight of terrorism programs.

I hope that this spirit of bi-partisanship continues this morning so that we can go about the serious business of adopting the set of policies and laws that best protects the American public from terrorism will preserving our traditional rights and liberties as American citizens.

TESTIMONY OF ASA HUTCHINSON
UNDERSECRETARY FOR BORDER AND TRANSPORTATION SECURITY
DEPARTMENT OF HOMELAND SECURITY
BEFORE THE SENATE JUDICIARY COMMITTEE
August 19, 2004

Chairman Hatch, Ranking Member Leahy, and other distinguished members. It is a pleasure to appear before you today to discuss how the Department of Homeland Security (DHS) is addressing the recommendations from the September 11 Commission Report relating to law enforcement, border security, and the USA PATRIOT Act.

As this Committee and the American people know, since the terrible events of September 11th, our federal law enforcement agencies have been heavily focused on ferreting out terrorists and their supporters. The DHS law enforcement agencies, and its predecessors, have been relentlessly pursuing the terrorists and their financial trails while protecting the privacy interests and civil liberties of our citizens.

At DHS, we are actively sharing information with all relevant federal and state law enforcement agencies, State, territorial, tribal, and local officials, and the private sector, using information we learn every day to refine our analytical tools we use to help identify terrorists and their supporters before they can reach America's shores, and employing new and emerging technologies, such as biometrics, in innovative ways to secure America and to preserve its economic security.

The American people can be proud of our efforts and achievements. I am honored to lead, under the direction of Secretary Ridge, the largest law enforcement component of DHS and represent them here today.

The Challenge

The challenge that DHS faces is enormous. We share nearly 7,500 miles of land border with Canada and Mexico, across which more than 326 million people, 119 million motor vehicles, 11 million truck containers, and 2.5 million rail cars pass every year. We patrol almost 95,000 miles of shoreline and navigable waters, and 361 ports that see over 203,000 vessels, 9 million containers of cargo, and nearly 15 million cruise and ferry passengers every year.

We have some 445 primary airports and another 124 commercial service airports that see 30,000 flights and 1.8 million passengers every day. There are approximately 110,000 miles of highway and 220,000 miles of rail track that cut across our nation, and 590,000 bridges dotting America's biggest cities and smallest towns.

Every day, our job is to work to make our country more secure. We are constantly evaluating our intelligence and a threat environment that literally changes by the hour and day.

Even in this ever-changing environment, however, we believe that terrorists will consistently target certain sectors and consistently look to use certain types of attack. That knowledge allows us to operate at a high level of awareness.

9/11 Commission Recommendations

Let me address the recommendations of the 9/11 Commission that are most relevant to this Committee and this hearing.

Targeting Terrorist Financing

The 9/11 Commission noted that, "[v]igorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us to understand their networks, search them out, and disrupt their operations."

DHS fully agrees.

Since the day DHS came into existence, we have continued the exemplary work of the former U.S. Customs Service to investigate terrorist financing schemes.

Unprecedented Interagency Cooperation

We have worked in close cooperation with the FBI on these cases. In an unprecedented exchange of information sharing between federal law enforcement agencies, our Bureau of Immigration and Customs Enforcement (ICE) vets all of its terrorist financing leads through the FBI pursuant to a Memorandum of Agreement (MOA) between DOJ and DHS.

ICE and the FBI have established a Joint Vetting Unit staffed by senior personnel from each agency to identify investigations with a potential nexus to terrorist financing. ICE has also detailed a senior-level manager to the FBI's Terrorist Financing Operations Center (TFOS) as the Deputy Section Chief. Thus, the FBI and DOJ are immediately aware of all ICE cases that relate to terrorist financing.

When an ICE investigation has a nexus to terrorism or terrorist financing, the investigating ICE field office is instructed to contact the appropriate FBI field office to arrange for a smooth transition of the investigation to the Joint Terrorism Task Force (JTTF).

ICE has also entered discussions with the Drug Enforcement Administration (DEA) about sharing information related to the counter-narcotics enforcement mission of each agency. DHS is seeking reciprocal access to FBI and DEA databases in order to strengthen the ability of DHS to perform its various missions more effectively and efficiently.

DHS and ICE have taken the fight against terrorist financing to the next level. The same weaknesses and vulnerabilities that organized criminal groups exploit today in our border security can be used tomorrow by terrorists and their supporters. Organized criminal groups who today smuggle narcotics or other commodities, like cigarettes or counterfeit merchandise, can tomorrow smuggle potential weapons of mass destruction using their existing networks. Similarly, groups who today specialize in smuggling undocumented aliens into the country can be used tomorrow to aid terrorists in evading inspection at the border.

Cornerstone

In response, ICE initiated the Cornerstone program to focus on the systems that criminals, including terrorist groups, alien smugglers, and Intellectual Property Rights (IPR) violators use to earn, store, and move their proceeds. Cornerstone is designed to identify potential vulnerabilities in our trade and financial systems that can compromise our economic security.

Through Cornerstone, ICE agents build partnerships and exchange information with the private businesses and industries that terrorists and other criminal organizations seek to use and exploit. This partnership enables ICE to provide timely information and feedback to the private sector so that they can take the appropriate precautions to protect themselves. ICE also receives information, tips, and insights from the businesses and industries that are the first to encounter and recognize possible indications of terrorist activity.

As part of Cornerstone and protecting the economic security of our homeland, ICE investigates money laundering related to banks and other traditional and non-traditional financial institutions, trade-based money laundering, the smuggling of bulk currency, the illegal use of money remitters and money service businesses, commercial fraud, IPR violations, cybercrime, and the illegal trade in weapons and dual-use goods and technology.

Targeting Terrorist Travel

The 9/11 Commission also stated that, "[t]argeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility."

We have implemented a number of successful programs to deny terrorists the ability to travel freely into the U.S., identify potential travel facilitators, and constrain the mobility of known and suspected terrorists.

The two I would like to focus on today are our creation and use of the National Targeting Center and our US-VISIT biometric screening system.

National Targeting Center

The NTC began around-the-clock operations on November 10, 2001, providing tactical targeting and analytical research support for the anti-terrorism efforts of the former-U.S Customs Service. The NTC is primarily staffed by DHS's Bureau of Customs and Border Protection (CBP). The NTC staff consists of CBP officers and field analysis specialists who are experts in passenger and cargo targeting for air, sea, and land operations in the inbound and outbound environments. The NTC develops tactical targets – potentially high-risk people and shipments that should be subject to a CBP inspection – and it develops these targets from raw intelligence, trade, travel, and law enforcement data.

NTC supports DHS field elements, here and overseas, including Container Security Initiative (CSI) personnel stationed in 21 countries throughout the world, the Visa Security Program, the Immigration Security Initiative[1], currently operated out of Schiphol Airport in Amsterdam, and to CBP Officers at all of our ports of entry, as well as between the ports through support to CBP's Office of Border Patrol.

During the period of heightened alert last December, the NTC played a pivotal role in analyzing passenger manifest information related to several international flights that were determined to be at risk, in order to ensure that passengers on board did not pose risks to the flights.

The NTC includes representatives from ICE, the FBI, the intelligence community, the Transportation Security Administration (TSA), US-VISIT, the Department of Energy, the Department of Agriculture, the Food and Drug Administration, and the United States Coast Guard.

The NTC uses the Automated Targeting System (ATS) to identify and target high-risk passengers and cargo entering the United States. ATS permits the NTC's trained personnel to process advance passenger information, to recognize anomalies and "red flags" and to determine which individuals and shipments should be given greater scrutiny at our ports of entry.

CBP continues to work on a version of ATS that, for the first time, will be able to identify potentially high-risk travelers in passenger vehicles. The new version of ATS will also increase the amount of government data that the system can access and analyze and enable us to train more people on the use of the system.

These, and many other U.S. intelligence analysis capabilities, are being used to help exploit terrorists' vulnerabilities as they travel and to learn more about their activities and methods. In addition to our ongoing efforts to target terrorist travel to, from, and within the United States, the Administration is seeking, on both a bilateral and multilateral basis,

[1] Under the Immigration Security Initiative (ISI), CBP will deploy teams of CBP Officers to overseas airports to work with local authorities in preventing the onward movement of people identified as presenting a security threat to the carrier or passengers on international flights destined to the U.S.

to promote similar efforts by other responsible governments, and to provide those governments with relevant terrorist-related information.

US-VISIT

Prior to the terrorist attack on September 11, Congress twice mandated the creation of an electronic entry-exit system. Following the events of September 11, Congress added the requirement that the entry-exit system incorporate biometric technology as a means to verify the identity of foreign travelers. DHS established the US-VISIT program ahead of schedule, and began operating US-VISIT at 115 ports of entry on January 5, 2004.

US-VISIT enhances the security of our citizens and visitors; facilitates legitimate travel and trade; ensures the integrity of our immigration system; and protects the identities and privacy interests of our visitors.

In addition to developing an integrated system that records the arrivals and departures of travelers and uses biometric technology to combat fraud, DHS designed US-VISIT to: (1) provide information to CBP Officers[2] and consular officers for decision making purposes; (2) reflect any pending or completed immigration applications or actions; (3) identify nonimmigrant overstays; and (4) provide accurate and timely data to appropriate enforcement authorities. US-VISIT accomplishes all these objectives.

US-VISIT represents a major milestone in enhancing our nation's security and our efforts to reform our borders. It is a significant step towards bringing integrity back to our immigration and border enforcement systems. It is also leading the way for incorporating biometrics into international travel security systems.

Integrated Entry-Exit System

US-VISIT is a continuum of security measures that begins before individuals enter the United States and continues through their arrival and departure from the country. Enrolling travelers in US-VISIT using biometric identifiers allows DHS to:

- Conduct appropriate security checks: We conduct checks of visitors against appropriate lookout databases and selected criminal data available to consular officers and CBP Officers at the ports of entry, including biometric-based checks, to identify criminals, security threats, and immigration violators.
- Freeze identity of traveler: We biometrically enroll visitors in US-VISIT – freezing the identity of the traveler and tying that identity to the travel document presented.
- Match traveler identity and document: We biometrically match that identity and document, enabling the CBP Officer at the port of entry to determine whether the traveler complied with the terms of her/his previous admission and is using the same identity.

[2] CBP Officers were formerly known as inspectors.

- Determine overstays: We will use collected information to determine whether individuals have overstayed the terms of their admission. This information will be used to determine whether an individual should be apprehended or whether the individual should be allowed to enter the U.S. upon her/his next visit.

The DHS and Department of State (DOS) together have created a continuum of identity verification measures that begins overseas, when a traveler applies for a visa, and continues upon entry and exit from this country. The system stores biometric and biographic data in a secure, centralized database and uses travel and identity documents to access that information for identity verification and watchlist checks. Today, more than 180 nonimmigrant visa-issuing posts and 90 immigrant visa issuing posts capture fingerscans and digital photographs of foreign nationals when they apply for visas, regardless of their country of origin. This process will be in place at all 211 visa-issuing posts worldwide within 60 days. In addition, on September 30, 2004, nationals from Visa Waiver Program (VWP) countries will be enrolled in US-VISIT when they travel to the United States.

At assigned U.S. border points of entry, designated visitors are required to provide biometric data, biographic data, and/or other documentation. This data is checked against various databases, which US-VISIT has successfully integrated and which contain visa issuance information, terrorist and criminal watchlists, and immigration status information. That information allows a CBP Officer at the border to verify the identity of the traveler and to determine whether the foreign national is a public threat or is otherwise inadmissible. In its first 7 months of operation, DHS processed nearly 7.3 million foreign national applicants for admission through US-VISIT at its air and sea ports of entry. During that period, 674 individuals were identified by biometrics alone as being the subject of a watchlist lookout.[3]

Our experience with biometrics is demonstrating that our ability to identify who entered and left the country is significantly improved with the addition of biometric identifiers. Here are some examples of US-VISIT intercepts:

- At Newark international airport, an international traveler appeared for inspection. Standard biographic record checks using a name and date of birth cleared the system without incident. However, a scan of the traveler's index fingers, checked against the US-VISIT biometric database, revealed that the traveler was using an alias and was, in fact, a convicted rapist. Additionally, he had previously been deported from the United States. US-VISIT's search disclosed that the individual used at least nine different aliases and four dates of birth. He had previously been convicted of criminal possession of a weapon, assault, making terrorist threats, and rape.

[3] Pursuant to immigration laws, DHS took adverse action in 35 percent of the 674 cases. Not all criminal violations make an alien inadmissible to the United States, and some aliens apply for and receive waivers of inadmissibility. Of the 674 hits, 64 percent were for criminal violations (some of which were immigration related criminal violations, such as previous deportation), and 36 percent were for immigration violations alone.

- CBP Officers at JFK International Airport processing a passenger through the US-VISIT procedures found that the individual was using an alias. Further information uncovered two arrests for aggravated trafficking of drugs, a subsequent failure to appear, and visa fraud. The traveler had used this fraudulent visa to enter the United States over 60 times without being detected by standard biographic record checks, the last time only 11 days earlier.
- Recently, a traveler with four aliases, three social security numbers, and a criminal history going back to 1990, tried to enter the United States. He was not admitted because a comparison of his fingerscans against the US-VISIT biometric watch list determined that he had previously been deported from the United States.

As these examples demonstrate, US-VISIT works.

Monitoring the status of visitors while in the United States is an integral part of border management and ensures the integrity of the immigration system. One of the US-VISIT Program's primary roles in status management is identifying those individuals who have overstayed the terms of their admission – calculated through the exchange of information from appropriate case management systems, especially those managed by U.S. Citizenship and Immigration Services (CIS). Incorporating biometrics into US-VISIT allows us to positively identify individuals who have overstayed their admission and gives DHS the ability to identify immigration benefits and visa fraud by identifying individuals who try to misrepresent their status or their identity.

Currently, our exit procedures are based largely upon biographic departure information from carrier produced passenger manifests. We match this information with the admission information and identify those likely to have overstayed the terms of their admission. Our goal is to enhance our ability to match arrivals and departures by using biometrics. We are testing this with various pilot programs at Baltimore-Washington International Airport, the Miami Cruise Terminal, and Chicago O'Hare Airport. We plan to expand our pilot program to a total of 15 air and seaports over the next several months. Through the pilot programs, we will test different options and evaluate the results to identify the most effective, cost-efficient process.

US-VISIT is achieving success because of biometric technology – matching digital fingerscans against lookout, criminal history, and enrollment data makes US-VISIT more effective.

Deterring the Use of Fraudulent Documents

The Commission's report noted that terrorists use altered and counterfeit travel documents to evade detection. In the border and immigration enforcement arenas, biometric identifiers are tools that help prevent the use of fraudulent identities and travel documents. The purpose of the biometric identifier is to verify a person's identity in order to run criminal history checks and to ensure that an individual cannot apply and/or be granted benefits under different names. Biometric visas issued by the DOS to

travelers to the United States allow one-to-one matches, to verify that the person presenting the visa is the person who was issued the visa, and one-to-many matches, to ensure that the bearer is not the subject of a biometric lookout or enrolled in the system under another name. Like the biometric visa process, US-VISIT enrollment fixes a person's identity. When a VWP traveler enrolls in US-VISIT, the person's fingerprints will be electronically linked to the passport, thus preventing another person from using that passport by freezing identities at the border and ensuring that the person is not enrolled under another name.

Sharing US-VISIT Data

The information integrated by US-VISIT includes appropriate biographic, biometric (i.e. fingerscans and digital photographs), and other immigration-related information. This information is collected or verified at each contact with the individual. Sharing the information in a timely manner with appropriate decision makers, ensures that they can make the best decisions possible. These decision makers include consular officials from the Department of State; and Customs and Border Protection officers, Immigration and Customs Enforcement agents, and U.S. Citizenship and Immigration Services officers from the Department of Homeland Security and other appropriate law enforcement officials. The vast majority of individuals whose information we collect are legitimate travelers who comply with U.S. laws. US-VISIT has established a data-sharing environment that specifies the security, privacy-related, and retention requirements that must be implemented by entities using US-VISIT information on a routine basis to protect the information provided by these individuals.

Safeguarding the Personal Privacy of Our Visitors.

An obvious concern for all legitimate travelers is that criminals will use their lost or stolen travel documents to enter the United States. Biometric identifiers make it difficult for criminals to travel on someone else's travel documents. This is a significant benefit that US-VISIT delivers for the millions of legitimate travelers the U.S. welcomes each year.

We must continue to respect the privacy of our visitors. Because the data we now collect from foreign nationals is considered to be highly personal and potentially subject to abuse, DHS has taken the extraordinary step of applying aspects of the U.S. Privacy Act of 1974 to this group of foreign nationals. Our approach has garnered widespread praise from privacy advocates and the general population of foreign travelers coming to the United States as well as some of our closest allies. These stakeholders have made it clear in the press, and in comments sent to us, that they expect us to honor our commitment to take the necessary steps to only use the information for the purposes stated.

Although biometric identifiers in the form of photographs and fingerprints have long played a key role in securing our borders, manually matching this information is subject to high costs and slow performance. The advent of automated matching capability gives us the ability to improve matching performance and permit the deployment and use of

new technologies in new ways to help us freeze or fix identities of foreign nationals, improve document security, and deter illegal access. To maximize our return on investment, it is vital that federal agencies and associated industries, who are also responsible for the security of infrastructure, work together to create compatible systems. US-VISIT has established a successful track record in protecting the integrity of the immigration and border management enterprise, but we continue to be vigilant in achieving our mission and goals.

US-VISIT is critical to our national security, and its implementation is already making a significant contribution to the efforts of DHS to provide a safer and more physically and economically secure America. We recognize that we still have a long way to go. We will build upon the initial framework and solid foundation to ensure that we continue to meet our goals to enhance the security of our citizens and visitors while facilitating travel for the millions of visitors we welcome each year.

Safeguarding Personal Privacy in General

The September 11 Commission Report recommends the creation of a board within the Executive Branch to oversee the balance of information sharing and privacy protections. We are working with other agencies to consider this recommendation. I can speak to the successes we have seen within DHS on privacy protections.

DHS has the first statutorily mandated Privacy Officer who serves the Department in two capacities. First, she works directly with operational components across the entire Department to embed privacy practices into the technology and the business processes DHS uses to accomplish its mission. To support this intense integration, the Privacy Officer also places privacy officers in the field, working side by side with the staff of DHS components. Second, she investigates and oversees DHS adherence to existing privacy laws and reports to both the Secretary and separately to Congress on DHS challenges and successes with privacy compliance. Through this dual role, the DHS Privacy Officer builds solid privacy practices into the daily work of the Department and assists in building a long term strategy for balancing privacy and security into the future. In its Report, the 9/11 Commission speaks of the need for creativity. The creation and the work of the DHS Privacy Officer is one example of how DHS is taking a new approach to providing comprehensive and balanced security to the nation.

Here in DHS, we can show the effectiveness of a strong privacy officer at the agency level and the success that is achievable only through direct integration of privacy protections and operational work. Privacy is an issue that stretches across the entire government and as we continue to look at government-wide approaches to privacy, it is also important to see how productive agency-level privacy protections are.

Interagency Human Trafficking Center

Last month, DHS and the Departments of State and Justice established the Human Smuggling and Trafficking Center. The center is housed at the State Department and includes the participation of intelligence agencies.

The Center analyzes and disseminates information, and provides related support to law enforcement, intelligence, diplomatic, foreign assistance, and other entities that take action against the threats of human smuggling and trafficking and against criminal support for terrorist travel.

The Center is another measure that the Administration has taken to improve our ability to analyze and disrupt terrorist travel. We are optimistic about its possibilities.

Targeted Prosecutions

DHS has coordinated an interagency working group to assure the greatest level of situational awareness for threat reporting, preparedness and coordination at all levels of government for the next several months. As part of this effort, ICE, CBP, and the FBI are working closely with the Department of Justice and the various United States Attorneys' Offices to identify, investigate, and criminally prosecute aliens possessing fraudulent documents, making false statements, or committing other immigration violations, where there is a suspicion of a connection to terrorism or a particular compelling national security interest.

All U.S. Attorneys' Offices were asked to meet with DHS and FBI representatives in their districts to develop guidelines for effective prosecutions in these cases and to articulate clearly the terrorism and national security interest at stake. The goal of the initiative is to ensure that the federal agencies are referring cases where a criminal prosecution can be brought to prevent and disrupt terrorism not to increase the number of criminal prosecutions for immigration violations.

An Integrated Screening System

The 9/11 Commission also recommended that, "[t]he U.S. border security system should be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The President should direct the Department of Homeland Security to lead the common effort to design a comprehensive screening system, addressing common problems and setting common standards with system-wide goals in mind."

There is no one-size-fits-all system to screen all persons, at all times, for all purposes. Instead, DHS, other federal agencies, state and local agencies, and the private sector rely on multiple screening systems that serve unique functions. The systems we develop need not be the same, but they must be interoperable to the extent possible.

US-VISIT

Earlier, I described the border screening system that is used by US-VISIT. US-VISIT employs a continuum of security measures that begins before individuals enter the U.S. and extends through their departure from the country. At assigned U.S. border points of entry, designated visitors are required to provide biometric data, biographic data, and/or other documentation. This data is checked against various databases which contain visa issuance information, terrorist and criminal watchlists, and immigration status information allowing CBP Officers at the border to verify identity and identify criminals, security threats and immigration violators.

CBP and One Face at the Border

DHS has also unified our border inspection process under the Customs and Border Protection Officers, who are cross-trained to address immigration, customs, and agricultural inspection needs. We now have one face in one uniform where we used to have three.

CBP recently graduated the first class of officers who are trained to operate primary inspection in all three areas. These officers -- now trained in all three areas of inspection and armed with the best intelligence we have -- improve our ability to spot and stop terrorists quickly and keep them out.

Transportation Security Administration

It is very important to note progress already made by the U.S government in expanding the existing no-fly and selectee lists. Prior to 9/11, there were fewer than 100 names on the "no fly" list. Today, the Transportation Security Administration (TSA) provides carriers with "no fly" and "selectee" lists that have been dramatically expanded. Every day, intelligence and law enforcement agencies submit new names for consideration. This places a significant burden on air carriers, reservation systems and airline passengers, and we appreciate their efforts and patience as these lists are used and continue to expand. Continued expansion will be possible through the integration and consolidation of various watch lists by the Terrorist Screening Center (TSC), and as the U.S. Government is able to assume the responsibility for conducting the list comparisons.

After a significant review of TSA's proposed CAPPS II system, DHS is nearing completion of a next-generation passenger prescreening program that meets our goals of using the expanded no-fly and selectee lists to keep known or suspected terrorists off of planes; moving passengers through airport security screening more quickly; reducing the number of individuals unnecessarily selected for secondary screening, and most importantly, fully protecting passengers' privacy and civil liberties.

A revised program will likely incorporate the valuable lessons we have learned from existing passenger prescreening programs, remove the responsibility from air carriers for conducting watch list comparisons, and improve aviation security. We look forward to working closely with Congress, the privacy and civil liberties communities, and the

aviation community to implement a new passenger prescreening program in the most cost-efficient and least-intrusive manner possible.

This summer, TSA initiated a pilot program, the Registered Traveler program, to help identify low-risk travelers. This program will allow screening resources to be more efficiently focused on higher-risk travelers.

The goal of the Registered Traveler (RT) Pilot Program is to use biometric technology in conjunction with pre-screening security assessments to assess the potential for an expedited screening procedure for qualified individuals. The RT concept is based on the premise that a balanced combination of terrorist threat analysis, verification of identity at the security checkpoint, and better-targeted physical screening can improve security and customer service. The RT Pilot Program is designed to allow DHS to focus its security resources on travelers that are "less known."

The program also includes a Registered Armed Law Enforcement Officer component to verify the identity of law enforcement officers who are traveling while armed.

I am pleased to announce we have launched operations at four of our five pilot locations: Minnesota, Los Angeles, Houston, and Boston which began operations on this past Tuesday. Washington DC's Reagan National Airport will launch operations in the next few weeks.

Additional Steps

We are continuously reviewing the systems that we have in place, and those under development. Our first priority is to ensure that the screening system works as intended. But we are also looking to see whether the system we employ in one place, for one function, can be used elsewhere.

I am leading a study within DHS to review the entire range of biometric programs that the Department employs. We want to see if it is possible to integrate the various screening programs and improve the performance of our mission functions. We are reviewing whether information we obtain in one program can be shared with another – without compromising the privacy rights and civil liberties of the individuals screened. That work is fully consistent with the Commission's recommendation in this area, and I am hopeful that it will lead to more efficient and integrated screening processes.

DHS Efforts to Strengthen Identity

I have testified above about the steps DHS has taken to strengthen the identification system used at our borders. For the very first time in our country's history, we are able to verify, through the collection and analysis of biometric information, that the foreign visitor who applies for and obtains a visa in the name of "Bill Smith" is the same "Bill Smith" who arrives at a U.S. port of entry.

DHS has worked with other federal agencies, including the Social Security Administration, and non-profit agencies, such as the American Association of Motor Vehicle Administrators (AAMVA) on identity issues, including proposals to strengthen procedures that are used to issue identification documents.

AAMVA recently completed a two-year effort to develop a security framework for strengthening the security of state-issued driver's licenses and identification cards. The AMMVA membership has not yet had the opportunity to ratify the recommendations, and State legislatures have also not had the chance to study the framework and consider what steps they would need to take to comply with the recommendations.

DHS is carefully considering the framework and its proposals. DHS encourages the States to review the framework as soon as practicable, and to take the appropriate actions necessary to increase the security of their identity issuing process.

DHS encourages the appropriate state and local officials to discuss these issues with their State Homeland Security Advisors and Governors. Steps to strengthen identity documents should be made a part of each state's homeland security strategy.

We are monitoring developments closely in this area, and are willing to work cooperatively with the States.

USA PATRIOT Act

I would also like to note the importance of the various provisions of the USA PATRIOT Act to the work of DHS and the BTS law enforcement agencies.

The PATRIOT Act began to tear down the walls that prevented our policy makers from having the benefit of intelligence analyses that were based on all available information. The PATRIOT Act has facilitated the ability of ICE, in coordination with the FBI, to query financial institutions quickly about terrorists and known money launderers. PATRIOT Act provisions have also enabled our investigators to investigate irregularities in the non-traditional financial system to close down unlicensed money remitters who may be funding terrorist activities. The PATRIOT Act has also expanded the authority of ICE to detain and remove terrorists from the United States.

I strongly support the President's call for Congress to renew those provisions of the Patriot Act that will otherwise expire next year. These tools are important as we build more integrated and coordinated homeland security, intelligence, and law enforcement communities.

Conclusion

I have described a number of steps that DHS has taken to improve our border screening and law enforcement efforts as a result of the September 11th terrorist attacks.

Our systems are better and more focused on terrorist prevention then they were before that fateful day. We can continue to improve the measures that we take and are committed to doing so.

The employees of DHS and the law enforcement agents, CBP Officers, air marshals, screeners, and others within my area of responsibility at the Directorate of Border and Transportation Security are working as hard as possible every day to prevent another act of terrorism. DHS is continuing to improve our understanding of the risks presented so that we can shift our resources as nimbly as possible to respond to the changing threat environment.

from the office of

Senator Edward M. Kennedy

of Massachusetts

FOR IMMEDIATE RELEASE
August 19, 2004

CONTACT: David Smith
(202) 224-2633

SENATOR EDWARD M. KENNEDY STATEMENT ON THE SENATE JUDICIARY COMMITTEE HEARING ON "THE 9-11 COMMISSION AND RECOMMENDATIONS FOR THE FUTURE OF FEDERAL LAW ENFORCEMENTAND BORDER SECURITY"

Mr. Chairman, thank you for calling this important hearing on the 9-11 Commission's recommendations for federal law enforcement and border security.

I commend Chairman Kean, Vice Chairman Hamilton and the other Commission members and their staffs for their extraordinary skill and dedication, their careful and detailed examination of the events leading up to that tragic day three years ago, and their thoughtful recommendations for reducing our vulnerability to similar terrorist attacks in the future.

A number of significant improvements have been made since 9/11, but no one would argue that the job of repairing the broken system of intelligence has been completed. The Commission has forcefully pointed out, as we give the Department of Justice, the Department of Homeland Security, and other agencies new responsibilities and new powers, we also need to focus on the privacy and civil liberties concerns raised by these changes.

The Commission found that we have no government-wide office assigned to monitor the protection of privacy and civil liberties, and it recommended a high level agency to meet that need. The DHS and the FBI are two of the agencies whose activities most demand that kind of monitoring, and I look forward to the views of our witnesses on how the new office should be structured.

Strengthening the security of our borders is a critical part of the ongoing effort to prevent future terrorist attacks. Some of the Commission's recommendations to improve border security are already being implemented, but others will require shifts in policy approaches before they can be carried out.

Our goal here is to strengthen the security of our borders without impeding the legitimate flow of people and commerce. More than 30 million foreign nationals enter the United States legally each year as tourists, students, or temporary workers. Over four hundred million visitors a year cross legally from Canada or Mexico to conduct their daily business or visit family members. The goal of our border screening system is to keep out those few who pose risk to our security, and to do so in a way that does not seriously undermine the efficient flow of legitimate border traffic that is an essential part of our national economy.

First, we need to move beyond the physical borders of the United States. We need to explore the concept of a North American perimeter as a single security unit.

The United States, Mexico, and Canada are closely linked by geography and by the legal flow of people, goods, services and trade of well over a billion dollars a day, and it makes sense for our three nations to act together to prevent terrorist attacks.

In the Border Security Act in 2002, Congress asked the President to study the feasibility of a North American National Security Perimeter, and we are still waiting for this report. As the 9/11 Commission's report states, "the U.S. government cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist information with trusted allies, and raise U.S. and global border security standards for travel and border crossing over the medium and long term through extensive international cooperation. "

Our consular officers and U.S. inspectors at airports overseas are essential parts of our border security as well. With accurate intelligence and appropriate training, consular officers and U.S. inspectors at airports can detect and intercept potential terrorists before they leave for the United States.

As the Commission stated, the "further away from our borders that screening occurs, the more security benefits we gain." The report recommends that some screening should occur before a passenger leaves on a flight for the U.S., and that we should work with other countries to ensure effective inspection procedures at as many airports as possible.

Currently, we have immigration inspectors at various airports in five nations, conducting reviews of immigration and travel documents and database checks of passengers waiting to board flights to the U.S. These pre-clearance sites should be expanded. A study of the feasibility of such an expansion was part of the Border Security Act as well, but we have not yet received a report from the Administration.

Another important area that needs immediate attention is the use of technology to identify potential terrorists. The Commission recommends a consolidated information network with watch list information and a biometric entry-exit screening system as

quickly as possible, with real-time access to immigration files and accurate intelligence on terrorists.

This system was mandated by the Border Security Act, and is now in varying stages of implementation. The Commission's report urges the rapid completion of this system, now known as US-VISIT, and the report also recognizes the major and expensive challenges to be overcome. Substantial funding is needed to replace antiquated computer systems and incorporate biometric features, and this funding is an essential investment in our national security.

Since these changes can cause significant delays at busy ports of entry, the challenge is to implement them expeditiously in a way that avoids serious slowdowns or breakdowns. We also need to make sure that the current infrastructure is adequate to accommodate the demands of an entry-exit system. Many ports may need additional lanes, staff and resources, and immigration inspectors must be trained in complex immigration laws, new technology, and various databases. Civil liberty and privacy concerns have to be addressed here. Adequate security protections are needed to protect against unreasonable data-sharing and identity theft. Effective guidelines are needed for the use of the information by government officials, with penalties for abuses, and the system must assure the quality and accuracy of the watch list databases.

As the 9/11 Commission found, our government has access to a vast amount of information, but current systems are weak for processing and using that information, especially across agency lines. Agencies live by the "need to know" rule and refuse to share. And each agency has its own computer systems and security practices.

The failure of the CIA and FBI to communicate with each other led to missed opportunities to prevent the 9/11 attacks. The CIA and FBI failed to include at least two hijackers, and possibly a third, on a timely watchlist. Had they been listed, the State Department would not have granted visas and the INS would not have allowed them to enter the United States.

As an example of what can be done to improve information sharing, the Commission recommends the establishment of a decentralized network that integrates data systems, but this is no easy challenge. Currently, from system to system and watch list to watch list, there is no standard for names, dates of birth, nationality, or biometric identifiers. We know that overall progress is being made. We have begun to eliminate some of the pre-9/11 obstacles that prevented the sharing of intelligence and law enforcement information with frontline agencies. The Attorney General and the FBI are now required to provide access by the State Department and the Homeland Security Department to criminal history records. The Border Security Act also mandated the creation of a data system with sophisticated name-search capabilities.

The Terrorist Screening Center is consolidating terrorism watchlist information into a single terrorism screening database, accessible to consular officers, immigration officials, and law enforcement officers through a 24/7 call-in center. The State

Department's TIPOFF lookout system has the most advanced and complete terrorist watchlist, and it has become part of the consolidated database.

I look forward to receiving an update from our witnesses about the implementation of all of these reforms, and also about steps being taken with respect to the protection of privacy and civil liberties. The Commission has provided an outstanding service to the nation with its comprehensive and thoughtful recommendations, and we have a responsibility in Congress to implement them as quickly and effectively as possible.

###

Opening Statement of Patrick Leahy
Hearing by the Senate Judiciary Committee
"The 9-11 Commission and Recommendations
For the Future of Federal Law Enforcement
And Border Security"
August 19, 2004

I commend the Chairman for arranging this hearing and I thank him for his accommodations in scheduling it.

I want to thank and welcome each of our witnesses, particularly my old friends Lee Hamilton and Slade Gorton. And let me say that as the Commission's chair and vice chair, Governor Kean and Congressman Hamilton offered extraordinary leadership in guiding this investigation through difficult shoals and bringing the Commission to its constructive and unanimous findings and recommendations. I have heard the high praise that you and other Commissioners have had for the Commission's staff, and I join you in that praise. The Report you together have produced is an exceptional product that deserves the Nation's attention, and it deserves the Congress's prompt consideration.

Decisions Facing ALL Americans

Senator Gorton once remarked that the commissioners checked their politics at the door, and the quality of the Commission's Report bears this out. By working so effectively in a non-partisan fashion, the 9-11 Commission has given us all a chance for a fresh start in tackling the issues the Report has identified. We should not squander that chance, and we should use the Commission as our model in striving for bipartisanship in making these decisions. After all, terrorists do not attack Democrats or Republicans or Independents; when they strike, they attack all of us as Americans.

I also want to commend the tireless efforts of the families and survivors of the 9-11 attacks, who fought so hard to ensure that this Commission was established. Like the commissioners, the victims groups put partisanship aside and pushed for an open, deliberate and accountable investigation, moving us forward in a constructive manner to better protect this Nation. Members of several victims groups are here today, and I want to personally thank them and welcome them here. I also want to submit for the record the written statement of Donald Goodrich of Bennington, Vermont. Mr. Goodrich, who lost his son, Pete, is the Chairman of Families of September 11. He could not be here today, but he has come to work closely with me on victims' issues, and I want to express my deep appreciation to him.

We cannot overstate the importance of oversight. I commend the Commission for fighting for full access to documents and official testimony, and for acknowledging in its final report the importance of open government. The report stated that secrecy can harm oversight, noting that democracy's best oversight mechanism is public disclosure.

Today's hearing will focus on two areas of great significance in this Committee's oversight jurisdiction: FBI reform and border security. Both are topics that are well-known to this Committee and that have been of particular concern to me. With my home state of Vermont sharing 90 miles of our international border with Canada, I am familiar with the challenges and concerns facing us in securing our borders after September 11.

FBI On The ABCs

The attacks of 9-11 did not create the problems the Commission has identified; they simply brought them into sharp relief. As someone who comes from a law enforcement background, several of them are problems that have concerned me for some time, and I know that they have concerned others on this Committee. Addressing some of these deficiencies was my first and my highest priority when I became chairman of the Judiciary Committee just a few months before September 11.

During that summer, it was already clear that the FBI over the years had lost its way on some of the fundamentals – the ABCs, if you will – starting with Accountability; Basic tools like computers, technology and translators; and "Culture" issues, like the treatment of whistleblowers and a resistance to sharing information outside the Bureau.

We began bipartisan hearings on reforming the FBI just weeks before September 11, and a new FBI Director pledged his commitment to correcting these longstanding problems. Director Mueller has made significant progress on several fronts, but the Commission's Report strikes several familiar chords, showing that there is much ground yet to cover before we can say that the FBI is as effective as Americans need the Bureau to be in preventing and combating terrorism. We continued the hearings on FBI reform after September 11th, and we sharpened our focus on the relevance of these longstanding problems to the newly declared war on terrorism. Our inquiry constituted the most intensive FBI oversight in many years, and it generated wide-ranging, bipartisan recommendations for reform.

The Commission Report identified many of the same failures within the FBI that we had highlighted in those hearings. It recognized, as do I, that Director Mueller has already taken certain steps to solve structural problems, and that, perhaps most important, he is striving to change the culture within the Bureau. These are important steps, but as the Commission pointed out, we need to ensure that changes put into place now will survive the current leadership of the Bureau and its component parts. Past attempts at FBI reform have died on the vine through lapses in leadership and lax congressional oversight.

Inadequate FBI Tools and Technology

I want to discuss two particular areas that gravely concern me: the FBI's foreign language translation program, and its information technology systems. These are the nuts and bolts of effective law enforcement and counter-intelligence, but we know now that in the months leading up to September 11th they were in sorry shape. Three years and many millions of dollars later we need to know what progress has been made and what more remains to be done.

Our FBI witness, Maureen Baginski, said recently that she was optimistic about the status of the FBI's foreign translation program, and I hope that she can share some good news with us today. Last spring, despite claims of "near real time" translation of wiretaps, the FBI could not state with any certainty how much time passes between the time a telephone call is taped and when it is translated. Is there still a vast backlog of material needing to be translated? The FBI sought an unprecedented number of new FISA wiretaps last year; how is this impacting critical FBI resources?

The FBI's longstanding problems in mastering the computer technology that is essential to modern-day law enforcement has been another great failing. The Trilogy solution, by all accounts, has been a disaster. By now, two phases of Trilogy have been completed, and all agents at last have their own computers and can send e-mails to one another. Of course, this is hardly a noteworthy accomplishment in the information age — especially $500 million to $600 million later.

What troubles me most, however, is that FBI agents are still trying to "connect the dots" using pencil and paper. The long-anticipated Virtual Case File System – which would at last put intelligence at the fingertips of the agents in the field -- is far behind schedule and vastly over budget. VCF should have been operational long ago, but the completion date keeps getting extended. In May, Director Mueller assured us that VCF would be deployed by the end of the year. But a month later – in June – we were told there would be further delays. By the time VCF is finally implemented, will it be "state of the art" or dreadfully outdated?

There are other critical areas in need of reform within the FBI. Some we learned about from the 9-11 Commission, some we learned about from our own oversight efforts and in reports by the DOJ Inspector General. But some critical problems have come to light only through the courageous voices of whistleblowers. Senator Grassley and I spend a great deal of time listening to reports from whistleblowers because we firmly believe that they may provide us with information critical to our national security. As a result of Enron and related corporate scandals, I worked with Senator Grassley and others in Congress to give broad protection to whistleblowers in the private sector, but, incredibly, Congress has not acted to protect those who come forward from the FBI to report problems that might impact our ability to prevent terrorist attacks.

The FBI Reform Act that Senator Grassley and I introduced in July 2003 is drawn from the FBI Reform Act that had been unanimously approved by this Committee a year

before, only to die on the Senate floor by an anonymous hold on the other side of the aisle. It addresses several outstanding problems in the Bureau, and acting on these reforms is long overdue. Among other things, the FBI Reform Act would protect FBI whistleblowers from retaliation and greatly improve congressional oversight of the Bureau.

Striking A Balance On Border Security

The Commission's report includes sobering evidence suggesting that three years after the attacks, our borders are not nearly as secure as they should be. As a Senator from Vermont, I know how important border security issues are to my constituents and the urgency both they and I feel about acting to protect our borders.

Let me be clear: I do not believe that America's response to terrorism should be to close our borders and isolate ourselves from the world. To the contrary, it is in our national interest to have visitors from around the world have positive experiences in the United States, and to go back home to tell their friends and neighbors about the beauty of our land, the fairness of its people and the vitality of its democratic principles. It is also in our national and economic interest to promote legal immigration to our country. If we are going to have an immigration policy that embraces the world, however, we need to be smarter about the way we police our borders, and I believe the report points us in a number of intelligent directions.

First, I could not agree more with the Report's review of this Congress' pre-9-11 treatment of the Northern Border. While our Southwest border was patrolled by four Border Patrol agents for each mile of border, our border with Canada had only one agent for every 13.25 miles. Even after we had evidence that terrorists were seeking to enter the United States from Canada, Congress turned a deaf ear to the needs of the Northern Border. It was only after the September 11 attacks that Congress finally acted, approving my proposal in the USA PATRIOT Act to triple the number of Border Patrol agents, INS Inspectors, and Customs agents stationed at our border with Canada. Even then, the Administration dragged its feet implementing the language, and years more passed before the tripling was finally achieved. Now that it has, I look forward to hearing from the Commissioners what additional steps should be taken to police the Northern Border.

Second, I applaud the Commission's focus on the issue of tracking terrorist travel. The Commission believes that if we had a system in place before 9-11 that analyzed terrorists' travel strategies, we might have intercepted between four and 15 of the hijackers. Since the attacks, a terrorist travel intelligence collection and analysis program has been put in place, and I agree with the Commission's recommendation that it be expanded. I also agree that frontline personnel at our consulates and our borders should receive training in spotting suspicious patterns of travel. Agents from our Customs and Border Patrol and Immigration and Customs Enforcement agencies should be trained to recognize suspicious travel documents, and we should have someone with document expertise at every port of entry and consulate.

Third, we should continue to work toward "expanding our borders" by placing more U.S. personnel in overseas airports, and working with other nations to share information more freely about persons who may pose a threat. "The further away from our borders that screening occurs, the more security benefits we gain," the Commission rightly states, arguing that "at least some screening should occur before a passenger departs on a flight destined for the United States." Additionally, if countries will share their own "watch lists" with our consular officers and our inspectors, we will gain additional leads about suspicious travelers. As the Commission puts it, "[e]xchanging terrorist information with other countries, consistent with privacy requirements, along with listings of lost and stolen passports, will have immediate security benefits." Enhancing this sort of coordination and cooperation— and securing the ability to operate in as many foreign airports as possible — are two of the many reasons why it is essential that we have leaders who can work closely and respectfully with other countries.

Finally, I agree with the Commission's recommendations that we "should complete, as quickly as possible, a biometric entry-exit screening system, including a single system for speeding qualified travelers." Our goal should be to have a U.S. VISIT system that screens foreign travelers as thoroughly as possible in the shortest possible time. Biometric capabilities promise to enhance our security procedures, and substantial efforts are underway. We already collect biometric information as part of U.S. VISIT. In addition, the U.S. has been involved in setting international standards for biometric passports for foreign visitors as well as U.S. citizens—a process that will likely set the stage for a broader domestic biometric program. But I am concerned that the process to date for finalizing international standards has largely occurred outside of congressional and public view, in negotiations by U.S. representatives and others in the International Civil Aviation Organization. This is troubling because technology and deployment choices will determine whether we have an effective screening system that is not only secure, but also adequately protects privacy and civil liberties. There are many issues to consider and much work to be done before such a system can be deployed, and Congress should be involved and invest in this process. I recently sent several questions to DHS requesting details on its biometric screening plans and will include them in today's record. I look forward to hearing about those details.

Support All States Rather Than Pit Large Against Small

The Commission recommended that homeland security assistance be "based strictly on an assessment of risks and vulnerabilities." But the 9/11 report did not suggest any specific changes in homeland security funding formulas.

I understand the Commission's frustration with the current level of homeland security assistance. I am frustrated too. But I believe the real problem is that the Bush Administration and Congress have failed to provide enough overall funding for first responders, and as a result the states are fighting over insufficient resources. The Hart-Rudman Terrorism Task Force Report found that our nation will fall approximately $98.4 billion short of meeting critical emergency responder needs through this decade's end if current funding levels are maintained.

We should be looking to increase the funds to our nation's first responders. But instead President Bush proposed cutting $800 million to our police, fire and rescue squads in this year's budget by reducing overall first responder funding from $4.3 billion last year to only $3.5 billion this year. Shortchanging our nation's first responders will not make us a safer nation.

I strongly believe that every state – rural or urban, small or large – has basic domestic security needs and deserves to receive Federal funds to meet those needs. After the terrorist attacks of September 11, 2001, we worked together to try to meet the needs of all state and local first responders from both rural and urban areas. Our fire, police and rescue teams in each state in the nation deserve support in achieving the new homeland security responsibilities the Federal government demands. Indeed, the Commission recognized this fact in their report when they declared that: "We understand the contention that every state and city needs to have some minimum infrastructure for emergency response."

All states, including smaller states, have basic needs in equipping their first responders. Larger states have even greater needs. Instead of pitting large states against small states, as the Administration has done by shortchanging overall resources for first responders, the needs of both should be recognized and addressed. These funds help police, fire and rescue squads meet the new homeland security responsibilities the federal government is asking them to meet.

Conclusion

The Commission rightfully found that Congress must subject itself to dramatic changes to strengthen government accountability. Specifically, I acknowledge the Commission's pointed rebuke to Congress about the need to engage more proactively in its constitutional oversight function. I have always believed in open and accountable government — including vigorous oversight — and will continue my support of this critical function of the U.S. Congress.

The Commission has rendered to history its careful reconstruction and analysis of the events of September 11th. The Commission has given to us the task of carefully considering its recommendations, drawn from those events – recommendations that, in several ways, would help the FBI get back to mastering its ABCs. We owe our fellow citizens, and the families of those whose lives were lost or forever changed by those attacks, our full and respectful consideration of these findings and these recommendations.

#####